



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

Port Security Strategy 2012

by

LT Morgan Ames	ENS Andrew Cole	Mr. Horng Leong Lim
ENS Yilei Liu	ENS Alan Marsh	Mr. Henry Nguyen
ENS Laura Okruhlik	LCDR Joseph Torian	
Mr. Chun Man Chan	MAJ Kim Chuan Chng	LCDR Dale Johnson
MAJ Kiah Wen Kwai	Mr. Kim Leng Koh	Mr. Thiow Yong Lim
LT Claude McRoberts	Mr. Chee Wai Ng	Mr. Chee Wan Ng
Mr. Min Yew Ng	Ms. Pei Tze Oh	Mr. Kar Leong Ong
Mr. Lin Kiat Peh	MAJ Wei Ting Soh	MAJ Chee Leong Tan
Mr. Leng Huei Toh	MAJ Yi Jim Wong	

15 June 2007

Approved for public release; distribution is unlimited

Prepared for: Wayne E. Meyer Institute of Systems Engineering
Naval Postgraduate School
777 Dyer Road, Code 97
Monterey, CA 93943

THIS PAGE INTENTIONALLY LEFT BLANK

NAVAL POSTGRADUATE SCHOOL
Monterey, California 93943-5000

Daniel T. Oliver
President

Leonard A. Ferrari
Provost

This report was prepared for the Meyer Institute of Systems Engineering, Naval Postgraduate School, 777 Dyer Rd., Monterey, CA 93943.

Reproduction of all or part of this report is authorized.

This report was prepared by Systems Engineering and Analysis Cohort 11 (SEA-11):

LT Morgan Ames
ENS Andrew Cole
Mr. Horng Lim
ENS Yilei Liu
ENS Alan Marsh
Mr. Henry Nguyen
ENS Laura Okruhlik
LCDR Joseph Torian

Reviewed by:

EUGENE P. PAULO
SEA-11 Project Advisor

RICHARD D. WILLIAMS
SEA-11 Project Advisor

Released by:

WAYNE P. HUGHES, JR.
Chair, Systems Engineering and
Analysis Curriculum Committee

DAN C. BOGER
Interim Associate Provost and
Dean of Research

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE June 2007	3. REPORT TYPE AND DATES COVERED Technical Report	
4. TITLE AND SUBTITLE: Title (Mix case letters) Port Security Strategy 2012			5. FUNDING NUMBERS	
6. AUTHOR(S) Morgan Ames, Chun Man Chan, Kim Chuan Chng, Andrew Cole, Dale Johnson, Kiah Wen Kwai, Kim Leng Koh, Horng Lim, Thiow Yong Lim, Yilei Liu, Alan Marsh, Claude McRoberts, Chee Wai Ng, Chee Wan Ng, Min Yew Ng, Henry Nguyen, Laura Okruhlik, Pei Tze Oh, Kar Leong Ong, Lin Kiat Peh, Wei Ting Soh, Chee Leong Tan, Leng Huei Toh, Joseph Torian, Yi Jim Wong				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this report are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			12b. DISTRIBUTION CODE A	
13. ABSTRACT (maximum 200 words) U.S. Navy and commercial ships have been lucrative targets for terrorist organizations. Realizing that ships are most vulnerable while in-port, adequate measures must be employed by port facilities to ensure vessel security. Commercial and naval ports have been set as a national priority in Homeland Security Presidential Directive 13. A successful terrorist strike against a port could produce long-term economic impact. In an attempt to develop a system of systems to prevent and defeat terrorist attacks against foreign and domestic ports, this study approached the threat from three different aspects: terrestrial, seaborne, and internal. This report uses the Systems Engineering Design Process to define the problem, generate alternatives, model scenarios, and analyze results to produce feasible and cost-effective solutions. No single system can address all issues prevalent in the port security problem. The recommended solutions individually address specific threats, namely vehicle-borne improvised explosive devices, small boat swarm tactics, importation of contraband or weapons of mass destruction, and employee sabotage. Although each solution effectively increased port security, improved port security measures resulted in greater cost. Some solutions yielded only marginal gain in effectiveness with drastic increases in cost.				
14. SUBJECT TERMS Port Security, Maritime Domain Protection, Systems Engineering, Extend, Arena, MANNA, Force Protection, Port of Oakland, Port of Singapore, Container Screening, Sensor Performance, Intrusive Cargo Inspection, Commercial Port, Vehicle Borne Improvised Explosive Devices, Small Boat Swarm Tactics, Importation of Contraband of Weapons of Mass Destruction			15. NUMBER OF PAGES 497	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL	

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

U.S. Navy and commercial ships have been lucrative targets for terrorist organizations. Realizing that ships are most vulnerable while in-port, adequate measures must be employed by port facilities to ensure vessel security. Commercial and naval ports have been set as a national priority in Homeland Security Presidential Directive 13. A successful terrorist strike against a port could produce long-term economic impact. In an attempt to develop a system of systems to prevent and defeat terrorist attacks against foreign and domestic ports, this study approached the threat from three different aspects: terrestrial, seaborne, and internal. This report uses the Systems Engineering Design Process to define the problem, generate alternatives, model scenarios, and analyze results to produce feasible and cost-effective solutions. No single system can address all issues prevalent in the port security problem. The recommended solutions individually address specific threats, namely vehicle-borne improvised explosive devices, small boat swarm tactics, importation of contraband or weapons of mass destruction, and employee sabotage. Although each solution effectively increased port security, improved port security measures resulted in greater cost. Some solutions yielded only marginal gain in effectiveness with drastic increases in cost.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	BACKGROUND	1
	1. Port Security, Shipping, and Commerce	1
	2. National Directives.....	2
B.	PURPOSE.....	3
C.	CONCEPT OF OPERATIONS (CONOPS).....	4
D.	OPERATIONAL ENVIRONMENT	6
	1. Terrestrial Threats Group (TTG)	6
	a. <i>Boundaries of the Area of Operation</i>	6
	b. <i>Size of Area of Operations</i>	7
	c. <i>Port Topology and Characteristics</i>	8
	2. Regional Seaborne Threats Group (RSTG)	10
	a. <i>Port of Oakland</i>	10
	b. <i>Port of Singapore</i>	11
	c. <i>Naval Assets</i>	14
	3. Source Seaborne Threats Group (SSTG)	14
	4. Internal Personnel Threats Group (IPTG).....	16
E.	THREATS AND THREAT SCENARIOS	18
	1. Terrestrial Threats Group	18
	a. <i>Minor Threat Scenarios</i>	19
	b. <i>Major Threat Scenarios</i>	19
	2. Regional Seaborne Threats Group.....	21
	3. Source Seaborne Threats	22
	4. Port Internal Threats Group	25
D.	SCOPE	27
	1. Participants.....	27
	2. Organization	28
E.	METHOD	29
F.	CHRONOLOGY.....	30
II.	TERRESTRIAL THREATS GROUP	33
A.	PROBLEM DEFINITION	33
	1. Needs Analysis.....	33
	a. <i>System Decomposition</i>	33
	b. <i>Stakeholder Analysis</i>	35
	c. <i>Input-Output Model</i>	38
	d. <i>Functional Analysis</i>	41
	2. Objectives Hierarchy	42
B.	DESIGN AND ANALYSIS	47
	1. Alternatives Generation	47
	a. <i>Truck Running Fence Scenario</i>	49

	<i>b.</i>	<i>Truck Running Gate Scenario</i>	<i>51</i>
	<i>c.</i>	<i>Truck Bombing Power Substation Scenario.....</i>	<i>52</i>
	<i>d.</i>	<i>IED Smuggled Through Gate Scenario.....</i>	<i>52</i>
	<i>e.</i>	<i>Radiological Weapons Scenario.....</i>	<i>54</i>
	<i>f.</i>	<i>Biological and Chemical Weapons Scenario.....</i>	<i>57</i>
	<i>g.</i>	<i>Terrorist Cell Importation Scenario.....</i>	<i>58</i>
	<i>h.</i>	<i>Sensor Solution Alternatives</i>	<i>59</i>
C.		MODELING AND ANALYSIS	70
	1.	Modeling Plan.....	70
	2.	Modeling Explanation	72
	3.	Analysis of Model Data.....	75
	<i>a.</i>	<i>In Depth Analysis of Effectiveness of Armed Guard.....</i>	<i>78</i>
	<i>b.</i>	<i>In Depth Analysis of Effectiveness of Spike Strips.....</i>	<i>82</i>
	<i>c.</i>	<i>In Depth Analysis of Effectiveness of Pop-up Barriers.....</i>	<i>85</i>
	<i>d.</i>	<i>Data Analysis Conclusions</i>	<i>88</i>
	4.	Cost Estimation	89
	<i>a.</i>	<i>Cost Estimate for Hardening Perimeter Fencing.....</i>	<i>89</i>
	<i>b.</i>	<i>Cost Estimate for Armed Guard</i>	<i>90</i>
	<i>c.</i>	<i>Cost Estimate for Spike Strips</i>	<i>91</i>
	<i>d.</i>	<i>Cost Estimate for Pop-Up Barrier</i>	<i>92</i>
	<i>e.</i>	<i>Cost Estimate for Concrete Blocks.....</i>	<i>93</i>
	5.	Cost Benefit Analysis	95
III.		REGIONAL SEABORNE THREATS GROUP	97
A.		PROBLEM DEFINITION	97
	1.	Needs Analysis.....	97
	<i>a.</i>	<i>System Decomposition</i>	<i>102</i>
	<i>b.</i>	<i>Stakeholder Analysis.....</i>	<i>102</i>
	<i>c.</i>	<i>Input-Output Model</i>	<i>104</i>
	<i>d.</i>	<i>Functional Analysis</i>	<i>105</i>
	2.	Objectives Hierarchy	108
B.		DESIGN AND ANALYSIS	110
	1.	Alternatives Generation	110
	2.	System Design Attributes	123
	3.	Feasibility Screening.....	128
C.		MODELING AND ANALYSIS.....	136
	1.	Proposed Detection and Tracking Systems for Modeling	136
	<i>a.</i>	<i>Sensor Design Considerations.....</i>	<i>137</i>
	<i>b.</i>	<i>Sensor Suite Concept of Operations.....</i>	<i>138</i>
	<i>c.</i>	<i>Sensor Consideration: Radar</i>	<i>138</i>
	<i>d.</i>	<i>Sensor Considerations: EO (IR/Thermal Imager)</i>	<i>142</i>
	<i>e.</i>	<i>Sensor Consideration: Acoustic Sensors</i>	<i>144</i>
	<i>f.</i>	<i>Coastal Patrol Routes.....</i>	<i>146</i>
	<i>g.</i>	<i>Possible Routes of Advancement for Small Boat Attacks ...</i>	<i>150</i>
	2.	Modeling Plan.....	151
	3.	Modeling Explanation	154

4.	Simulation Setup	168
a.	Key Simulation Parameters	169
b.	Limitations of the Current Simulation Engine	171
c.	Simulation Runs	171
5.	Results and Key Findings	174
a.	Current Configuration	174
b.	Current and USV (B)	176
c.	Current and USV and 1 Additional Radar (C)	177
d.	Current and USV and 2 Additional Radar (D)	179
e.	Current and USV and 2 Additional Radar and Thermo Vision Sentry II (E)	181
f.	Current and USV and 2 Additional Radar and Thermo Vision Sentry II and Thermo Vision Sentinel (F)	183
g.	Current and USV and 2 Additional Radar and Thermo Vision Sentry II and Thermo Vision Sentinel and Networked Sensors and Sonar (F)	185
h.	Key Findings	188
5.	Cost Estimation	190
6.	Cost Benefit Analysis	196
IV.	SOURCE SEABORNE THREATS GROUP	199
A.	PROBLEM DEFINITION	199
1.	Needs Analysis	199
a.	System Decomposition	199
b.	Stakeholder Analysis	200
c.	Input-Output Model	202
d.	Functional Analysis	204
2.	Objectives Hierarchy	208
B.	DESIGN AND ANALYSIS	213
1.	Alternatives Generation	213
a.	Considerations for Alternatives	213
b.	Status Quo Alternative	218
c.	Zero Percent Inspection Alternative	219
d.	100 Percent Volume Screening Alternative	219
e.	Improved Loading Inspection Alternative	221
f.	Minimum Port Operations Disruption Alternative	221
g.	High Performance Alternative	223
h.	100 Percent Intrusive Inspection Alternative	223
2.	System Design Attributes	224
3.	Feasibility Screening	224
C.	MODELING AND ANALYSIS	226
1.	Modeling Plan	226
2.	Modeling Explanation	227
a.	General Flow of Containers through Port Inspections	228
b.	General Assumptions for All Inspection Modules	229
c.	Process Flow for Container Generation	230

	<i>d. Process Flow for Fixed Point of Entry</i>	<i>230</i>
	<i>e. Process Flow for Yard (Non-Intrusive) Inspection</i>	<i>231</i>
	<i>f. Process Flow for Crane (Non-Intrusive) Inspection</i>	<i>231</i>
	<i>g. Process Flow for ATS and Random Inspection.....</i>	<i>232</i>
	<i>h. Process Flow for Intrusive Inspection</i>	<i>232</i>
3.	Model Inputs.....	233
	<i>a. Container Traffic</i>	<i>233</i>
	<i>b. Sensor Performance.....</i>	<i>234</i>
4.	Model Results and Analysis	236
	<i>a. Optimal Sensor Mix</i>	<i>237</i>
	<i>b. Partitioning Analysis.....</i>	<i>252</i>
	<i>c. Data Analysis Conclusions</i>	<i>260</i>
5.	Cost Estimation	262
	<i>a. Manifest Screening</i>	<i>262</i>
	<i>b. Scanning Location</i>	<i>263</i>
	<i>c. Non-Intrusive Container Screening.....</i>	<i>265</i>
	<i>d. Intrusive Container Screening</i>	<i>266</i>
	<i>e. Smart Tags.....</i>	<i>268</i>
	<i>f. Alternative Cost Analysis</i>	<i>268</i>
6.	Cost Benefit Analysis	270
V.	INTERNAL PERSONNEL THREATS GROUP	273
A.	PROBLEM DEFINITION	273
1.	Needs Analysis.....	273
	<i>a. System Decomposition</i>	<i>273</i>
	<i>b. Stakeholder Analysis.....</i>	<i>274</i>
	<i>c. Input-Output Model.....</i>	<i>277</i>
	<i>d. Functional Analysis</i>	<i>279</i>
2.	Objectives Hierarchy	282
B.	DESIGN AND ANALYSIS	285
1.	Alternatives Generation	285
C.	MODELING AND ANALYSIS	298
1.	Modeling Plan.....	298
2.	Modeling Explanation	300
	<i>a. Deterrence Model.....</i>	<i>300</i>
	<i>b. Physical Access Control Model</i>	<i>302</i>
	<i>c. Data Access Control Model</i>	<i>305</i>
	<i>d. Response Model.....</i>	<i>315</i>
3.	Modeling Results and Analysis	317
4.	Cost Estimation	326
5.	Cost Benefits Analysis.....	328
VI.	CONCLUSIONS AND RECOMMENDATIONS.....	331
A.	TERRESTRIAL THREATS GROUP	331
1.	Conclusions and Recommendations.....	331
2.	Areas of Future Study	332
B.	REGIONAL SEABORNE THREATS GROUP	332

1.	Conclusions and Recommendations.....	332
2.	Areas of Future Study	333
C.	SOURCE SEABORNE THREATS GROUP	334
1.	Conclusions and Recommendations.....	334
2.	Areas of Future Study	335
D.	INTERNAL PERSONNEL THREATS GROUP	336
1.	Conclusions and Recommendations.....	336
2.	Areas of Future Study	337
E.	PORT SECURITY STRATEGY BEYOND 2012.....	337
APPENDIX A: TTG MODELS		341
APPENDIX B: TTG MODELING RESULTS		343
APPENDIX C: TTG LIFE CYCLE COST DSC2000 BARRIER.....		345
APPENDIX D: TTG COST BENEFIT ANALYSIS		353
APPENDIX E: SSTG MODELS		357
APPENDIX F: SSTG METRICS		363
APPENDIX G: SSTG INPUT PARAMETERS.....		367
APPENDIX H: SSTG ALTERNATIVE PARAMETER SETTINGS		373
APPENDIX I: SSTG MODEL DATA ANALYSIS SUPPLEMENT.....		381
APPENDIX J: HARBORGUARD TEST PLAN		425
LIST OF REFERENCES		457
INITIAL DISTRIBUTION LIST		463

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1. Locations of Major U.S. Container Ports	2
Figure 2. Terminals at the Port of Oakland.....	7
Figure 3. Terminals at PSA Singapore	7
Figure 4. Tanjong Pagar and Brani Terminals.....	15
Figure 5. Shipping Lanes of Asia	16
Figure 6. Integrated Project Participants.....	27
Figure 7. Port Security 2012 Organizational Layout	28
Figure 8. TTG System Decomposition	34
Figure 9. TTG Input-Output Model	38
Figure 10. TTG Denial Functional Flow Diagram	41
Figure 11. TTG Deterrence Functional Flow Diagram	42
Figure 12. TTG Overall Objectives Hierarchy	43
Figure 13. TTG Deter Objectives Hierarchy	43
Figure 14. TTG Deny Objectives Hierarchy.....	44
Figure 15. VIDAlert CCTV System	59
Figure 16. Intelli-FLEX Network Configuration.....	60
Figure 17. Intelli-FIBERT Configuration.....	61
Figure 18. Permitrax System.....	61
Figure 19. Intelli-FIELD System	62
Figure 20. Intelli-WAVE System	62
Figure 21. RedFlex Lasercam System	63
Figure 22. RFID Cargo Tag.....	64
Figure 23. Fingerprint Identification (DHS IDENT System)	64
Figure 24. Hand Geometry Biometrics	65
Figure 25. Vehicle Explosive Detection Systems.....	65
Figure 26. Hand-Held Trace Detector	66
Figure 27. AVIAN Heartbeat Detector.....	66
Figure 28. X-Ray Scanners	67
Figure 29. Gamma Ray Scanners.....	68
Figure 30. Radiation Portal Monitors	68
Figure 31. TTG Gate Security Model.....	72
Figure 32. Simulation Results Based on Distance	76
Figure 33. Simulation Results Based on Type of Barriers.....	77
Figure 34. Effectiveness of Armed Guard Configurations at Various Ranges.....	79
Figure 35. Effectiveness of Armed Guards and Concrete Blocks at Various Ranges.....	80
Figure 36. Relative Effectiveness of Concrete Blocks with Armed Guards.....	81
Figure 37. Effectiveness of Spike Strip Configurations at Various Ranges	82
Figure 38. Effectiveness of Strike Strips and Concrete Blocks	83
Figure 39. Relative Effectiveness of Concrete Blocks Using Spike Strips	84
Figure 40. Effectiveness of Different Configurations of Pop-up Barriers.....	86
Figure 41. Effectiveness of Pop-up Barriers and Concrete Blocks	87

Figure 42. Relative Effectiveness of Concrete Blocks with Pop-up Barriers.....	88
Figure 43. Concrete Block Implementation.....	93
Figure 44. Concrete Block Effective Placement for 20 MPH Speed Limit.....	94
Figure 45. Cost vs Effectiveness of Alternatives.....	95
Figure 46. RSTG System Decomposition.....	102
Figure 47. RSTG Input-Output Model.....	105
Figure 48. RSTG Small Boat Threat Functional Flow Diagram	106
Figure 49. RSTG Large Ship Threat Functional Flow Diagram	107
Figure 50. RSTG Sea Inserts Threats Functional Flow Diagram	108
Figure 51. RSTG Objectives Hierarchy	109
Figure 52. Operating Environment for the Port of Singapore	123
Figure 53. Operating Environment for the Port of Oakland	125
Figure 54. Desired Detection and Engagement Range	128
Figure 55. Port of Oakland Detection Boundaries.....	137
Figure 56. Existing Radar Site	141
Figure 57. Additional Radar Site	142
Figure 58. Electro-Optics Sensors Deployment Plan	144
Figure 59. Acoustic Sensor Deployment Plan	146
Figure 60. Locations of the Vessel Routes and Marina	147
Figure 61. Patrol Routes 1 and 2 (Coastal Patrol)	148
Figure 62. Patrol Routes 3 and 4 (Anchorage Patrol).....	149
Figure 63. Threat Routes: Possible Advancement Routes from Near Bank Marinas.....	150
Figure 64. Threat Routes: Possible Advancement Routes from Far Bank Marinas	151
Figure 65. RSTG Model - Small Boat Procedure Flow Chart.....	154
Figure 66. RSTG Discrete Event Components.....	155
Figure 67. Scenario Controller of Port Security Local Waterside Model.....	157
Figure 68. Visual Simulation of Port Security Local Waterside Model.....	158
Figure 69. Vulnerable Take Off Point of Terrorist and Vessel Routes	161
Figure 70. Key Areas of the Port of Oakland	161
Figure 71. Route 1 of Threats	162
Figure 72. Route 2 of Threats	162
Figure 73. Route 3 of Threats	163
Figure 74. Route 4 of Threats	163
Figure 75. Route 5 of Threats	164
Figure 76. Route 6 of Threats	164
Figure 77. Encoding of Routes of the Patrol Crafts.....	166
Figure 78. Encoding of Routes of USV and Helicopter	167
Figure 79. Encoding of Positions and Coverage of the Radars	167
Figure 80. Encoding of Positions and Coverage of the Electro-Optics Sensors.....	168
Figure 81. Encoding of Positions and Coverage of the Acoustic Sensors.....	168
Figure 82. Scenario Controller for Simulation Engine	169
Figure 83. Designated Terrorist Target Area.....	170
Figure 84. Infiltration and Detection Rate for (A) Configuration	175
Figure 85. Infiltration and Detection Rate for (B) Configuration.....	176
Figure 86. Infiltration and Detection Rate for (C) Configuration.....	178

Figure 87. Infiltration and Detection Rate for (D) Configuration	180
Figure 88. Infiltration and Detection Rate for (E) Configuration.....	182
Figure 89. Infiltration and Detection Rate for (F) Configuration	184
Figure 90. Infiltration and Detection Rate for (G) Configuration	186
Figure 91. Terrorist Detection Rate for Various Sensor Configurations.....	188
Figure 92. Cost vs Detection for Alternatives A-G with Odd Number Terrorists.....	196
Figure 93. Cost vs Detection for Alternatives A-G with Even Number Terrorists	197
Figure 94. SSTG System Decomposition	199
Figure 95. SSTG Stakeholders.....	201
Figure 96. SSTG Input-Output Model.....	203
Figure 97. Deny Loading of Undesired Cargo Functional Flow Diagram	205
Figure 98. Ship's Crew Infiltration Functional Flow	206
Figure 99. Detect and Disrupt UAV Attack on Transiting Ship Functional Flow	206
Figure 100. Secure Chokepoint Loading to Port Functional Flow	207
Figure 101. Objectives Hierarchy for Deny Container Holding Undesired Cargo.....	209
Figure 102. Objectives Hierarchy for Detect and Disrupt UAV Attack.....	210
Figure 103. Objectives Hierarchy for Deny Terrorist Access Onboard Container Ship	211
Figure 104. Objectives Hierarchy for Secure Chokepoint Leading to Domestic Port.....	211
Figure 105: Handheld and Fixed Structure Radiation Detectors [49]	220
Figure 106. SSTG Simulation Model	228
Figure 107. Mallow's Cp.....	248
Figure 108. Minitab Results of New Model	249
Figure 109. Interval Plots for Gamma Detectors	250
Figure 110. Interval Plot of Inspection Station Sensors	251
Figure 111. Interval Plot of eScanPrc and ATS.....	252
Figure 112. Partition Tree for Probability of Detection (Max Pd, rightmost)	254
Figure 113. Partition Tree for False Alarm Rate (Min FAR, leftmost)	256
Figure 114. Partition Tree for Productivity (Max Productivity, rightmost)	257
Figure 115. Partition Tree for Inspection Time per Container (Min Time, leftmost)	259
Figure 116. Cost vs Utility Score of Alternatives.....	272
Figure 117. IPTG Stakeholders.....	275
Figure 118. IPTG Input-Output Model.....	277
Figure 119. IPTG Functional Hierarchy	279
Figure 120. IPTG Objectives Hierarchy for Operations.....	284
Figure 121. IPTG Objectives Hierarchy for Deter.....	284
Figure 122. IPTG Objectives Hierarchy for Access	284
Figure 123. IPTG Objectives Hierarchy for Response	285
Figure 124. Gate Access Flowchart.....	302
Figure 125. Unauthorized Movement Flowchart.....	303
Figure 126. Distribution of Arrival at Gate	304
Figure 127. System Level Network	306
Figure 128. Summary of Intruder Strategy and Probability of Success	307
Figure 129. Probabilistic Data Access Model.....	308
Figure 130. Bayes Rule.....	309
Figure 131. Probability of Success for Minimum Scenario.....	310

Figure 132. Probability of Success for Maximum Scenario	312
Figure 133. Physical Access Control EXTEND Model.....	318
Figure 134. MANA Model with Internal Fence	319
Figure 135. MANA Model Denoting Communication Links.....	320
Figure 136. EXCEL model of Data Access Control System.....	321
Figure 137. Cost Comparison of All Alternatives Analyzed	329
Figure 138. Time Comparison of All Alternatives Analyzed.....	330

LIST OF TABLES

Table 1. Physical Port Size for Port of Singapore and Oakland	8
Table 2. Defensive Barrier Employment	9
Table 3. Eastern Sector Anchorages Examples	13
Table 4. TTG Stakeholders	36
Table 5. Evaluation Metrics for TTG Objectives	46
Table 6. Terrestrial Threats Morphological Chart (Section 1)	48
Table 7. Terrestrial Threats Morphological Chart (Section 2)	48
Table 8. Terrestrial Threats Morphological Chart (Section 3)	48
Table 9. TTG Model Abbreviations.....	76
Table 10. Cost Estimation Table for Spike Strips.....	91
Table 11. Cost Estimation Table for Pop-Up Barriers.....	92
Table 12. Cost Estimation Table for Concrete Blocks	94
Table 13. Evaluation Metrics for RSTG Objectives.....	110
Table 14. RSTG Possible Platforms, Sensors, and Engagement Options	111
Table 15. RSTG Summary of Alternatives.....	121
Table 16. RSTG Proposed Port Security Architecture	122
Table 17. Sensor Suite Concept of Operations	138
Table 18. Radar Specifications	139
Table 19. Radar Specifications	140
Table 20. Electro-Optics/Infrared Specifications	143
Table 21. Acoustic Sensor Specifications.....	145
Table 22. Sensor Specifications Encoded in Port Local Waterside Simulation	165
Table 23. RSTG Sensor and Platform Configurations for Simulation	173
Table 24. Infiltration and Detection Rate for (A) Configuration.....	174
Table 25. Sensor Detection Rate for (A) Configuration.....	175
Table 26. Infiltration and Detection Rate for (B) Configuration.....	176
Table 27. Sensor Detection Rate for (B) Configuration	177
Table 28. Infiltration and Detection Rate for (C) Configuration.....	178
Table 29. Sensor Detection Rate for (C) Configuration	179
Table 30. Infiltration and Detection Rate for (D) Configuration.....	180
Table 31. Sensor Detection Rate for D Configuration.....	181
Table 32. Infiltration and Detection Rate for (E) Configuration	182
Table 33. Sensor Detection Rate for E Configuration	183
Table 34. Infiltration and Detection Rate for (F) Configuration	184
Table 35. Sensor Detection Rate for F Configuration	185
Table 36. Infiltration and Detection Rate for (G) Configuration.....	186
Table 37. Sensor Detection Rate for G Configuration.....	187
Table 38. Summary of Cost per Configuration.....	191
Table 39. Total Cost for Alternative A	192
Table 40. Total Cost for Alternative B	192
Table 41. Total Cost for Alternative C	193

Table 42. Total Cost for Alternative D	194
Table 43. Total Cost for Alternative E.....	194
Table 44. Total Cost for Alternative F.....	195
Table 45. Total Cost for Alternative G	195
Table 46. MOE/MOP for Deny Container Holding Undesired Cargo from Loading	209
Table 47. MOE/MOP for Detect and Disrupt UAV Attack on Transiting Container Ship ..	210
Table 48. MOE/MOP for Deny Terrorist Access Onboard Container Ship	211
Table 49. MOE/MOP for Secure Chokepoint Leading to Domestic Port	212
Table 50. Deny Loading of Undesired Cargo Feasibility Screening	226
Table 51. SSTG Type I and II Errors Defined.....	227
Table 52. Sensor Performance Inputs for Fixed Entry	235
Table 53. Sensor Performance Inputs for Non-Intrusive Inspection	235
Table 54. Sensor Performance Inputs for Intrusive Inspection.....	236
Table 55. Sensor Performance Inputs for Crane.....	236
Table 56. Station Format for Determining MOP Related to Accuracy	238
Table 57. Station Format for Determining MOP Related to Timeliness	238
Table 58. Results of Goodness of Fit Test.....	244
Table 59. Type III Sum of Squares for the 17 Factors.....	245
Table 60. Coefficients and Results of the stepAIC Function.....	247
Table 61. Cost of Improving the ATS System in 2001 Dollars.....	263
Table 62. Cost Estimation for Mobile Scanning System.....	264
Table 63. Cost Estimation for Fixed Scanning System	265
Table 64. Cost Estimation for Crane Spreader Scanning System.....	265
Table 65. Cost Estimation for Trained Animals	266
Table 66. Cost Estimation for Scales.....	266
Table 67. Cost Estimation for Portable Radiation Detector	267
Table 68. Cost Estimation for Customs Inspector	267
Table 69. Cost Estimation for remotely Operated Inspection Robots	268
Table 70. Number of Systems Used in Each Inspection Station	269
Table 71. Utilization of Servers at Inspection Stations for Each Alternative.....	269
Table 72. Cost Estimation for Six Alternatives	270
Table 73. Rank of Alternatives Based on Utility	271
Table 74. IPTG Evaluation Metrics	285
Table 75. IPTG Morphological Chart.....	287
Table 76. IPTG Model Input Parameters and Associated MOEs	299
Table 77. IPTG Model Activity Parameters	304
Table 78. Data for Network Nodes (Minimum Scenario)	309
Table 79. Probabilities of Detection for Possible Move (Minimum Scenario)	310
Table 80. Data for Network Nodes (Maximum Scenario).....	311
Table 81. Probabilities of Detection for Possible Moves (Maximum Scenario)	311
Table 82. Input Parameter for Minimum Scenario	313
Table 83. Results for Minimum Scenario Simulation	313
Table 84. Input Parameters for Maximum Design Scenario.....	314
Table 85. Results of Maximum Scenario Simulation	314
Table 86. Response Terrain Model Description	316

Table 87. MANA Model Attributes	316
Table 88. EXTEND Model Results	321
Table 89. MANA Raw Data Matrix	321
Table 90. Combined Physical Access & Response Model Results	323
Table 91. Psychological Deterrence of Implementing Access Control Measure	324
Table 92. Combined Total Probability Detection	325

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ABBREVIATIONS, ACRONYMS, AND SYMBOLS

2FA	Two Factor Authentication
ADS	Active Denial System
AIS	Automatic Identification System
AMS	Automated Manifest System
AMSC	Area Maritime Security Committee
APS	Aerosol Particle Sizer
ASV	Autonomous Surface Vessel
ATS	Automated Targeting System
AUV	Autonomous Underwater Vehicle
AVIAN	Advanced Vehicle Interrogation and Notification System
C2	Command and Control
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CBP	Customs Border Protection
CCTV	Closed Circuit Television
CO	Commanding Officer
COI	Contact of Interest
CONOPS	Concept of Operations
COP	Common Operational Picture
C-TPAT	Customs – Trade Partnership Against Terrorism
CIWS	Close In Weapon System
DDG	Guided Missile Destroyer
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DMZ	Demilitarized Zone
DoD	Department of Defense
EMP	Electromagnetic Pulse
EO	Electro-Optical

FAA	Federal Aviation Administration
FSO	Facility Security Officer
GT	Gross Tons
GUI	Graphical User Interface
HARTS	Harbor Craft Transponder System
HCSC	Harbor Craft Security Code
HF	High Frequency
HSAS	Homeland Security Advisory System
HSPD	Homeland Security Presidential Directive
HUMINT	Human Intelligence
IA	Information Assurance
ICA	Immigration & Checkpoint Authority
IED	Improvised Explosive Device
IFF	Identify Friendly or Foe
IMO	International Maritime Organization
IP	Internet Protocol
IPR	Interim Progress Review
IPTG	Internal Personnel Threats Group
IR	Infrared
ISPS	International Shipping & Port Facility Security
IT	Information Technology
LHD	Amphibious Assault Ship
LIDAR	Light Detection and Ranging
LNG	Liquefied Natural Gas
LPG	Liquefied Petroleum Gas
LRAD	Long Range Acoustic Device
MANA	Map Aware Non-Uniform Automata
MARSEC	Maritime Security
MDA	Maritime Domain Awareness
MMSI	Maritime Mobile Service Identity

MOE	Measures of Effectiveness
MOP	Measures of Performance
MOVES	Modeling, Virtual Environments and Simulation
MPA	Maritime Port Authority
MTFB	Mean Time Between Failure
MTSA	Maritime Transportation Security Act
NOLH	Nearly Orthogonal Latin Hypercube
NPS	Naval Postgraduate School
NPT	Non-Proliferation Treaty
NVMC	National Vessel Movement Center
OR	Operations Research
PA	Public Address System
PANS	Pre-Arrival Notification of Security
PDA	Personal Digital Assistants
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PCG	Police Coast Guard
PCSC	Pleasure Craft Security Code
PSS12	Port Security Strategy 2012
PSA	PSA Singapore Terminals
PSO	Port Security Officer
PSYOPS	Psychological Operations
PV	Patrol Vessels
QFD	Quality Functional Deployment
RCS	Radar Cross Section
RDD	Radiological Dispersal Device
RFID	Radio Frequency Identification
RHIB	Rigid Hull Inflatable Boat
ROE	Rules of Engagement
ROV	Remotely Operated Vessels

RPG	Rocket Propelled Grenades
RPM	Radiation Portal Monitor
RSN	Republican Singapore Navy
RSTG	Regional Seaborne Threats Group
SAR	Search and Rescue
SCDF	Singapore Civil Defence Force
SCG	Singapore Coast Guard
SEA	Systems Engineering and Analysis
SEDP	Systems Engineering Design Process
SOLAS	Safety of Life at Sea
SPF	Singapore Police Force
SSAS	Ship Security Alert System
SSL	Secure Socket Layer
SSTG	Source Seaborne Threats Group
STW	Singapore Territorial Waters
TEU	Twenty-foot Equivalent Units
TDSI	Temasek Defence Systems Institute
TTG	Terrestrial Threats Group
TSA	Transportation Security Administration
TWIC	Transportation Worker Identification Credential
UAV	Unmanned Aerial Vehicle
URC	United States Regulatory Commission
USD	U.S. Dollars
USV	Unmanned Surface Vessel
VIS	Vessel Identification System
WMD	Weapons of Mass Destruction

ACKNOWLEDGEMENTS

The students of System Engineering and Analysis Cohort Eleven Port Security Strategy 2012 Team would like to thank the following faculty and staff of the Systems Engineering Curriculum, Wayne E. Meyer Institute, Naval Postgraduate School, and Port of Oakland, Port of Singapore stakeholders for their instruction, dedication to excellence, and input which prepared us to complete this thesis project work.

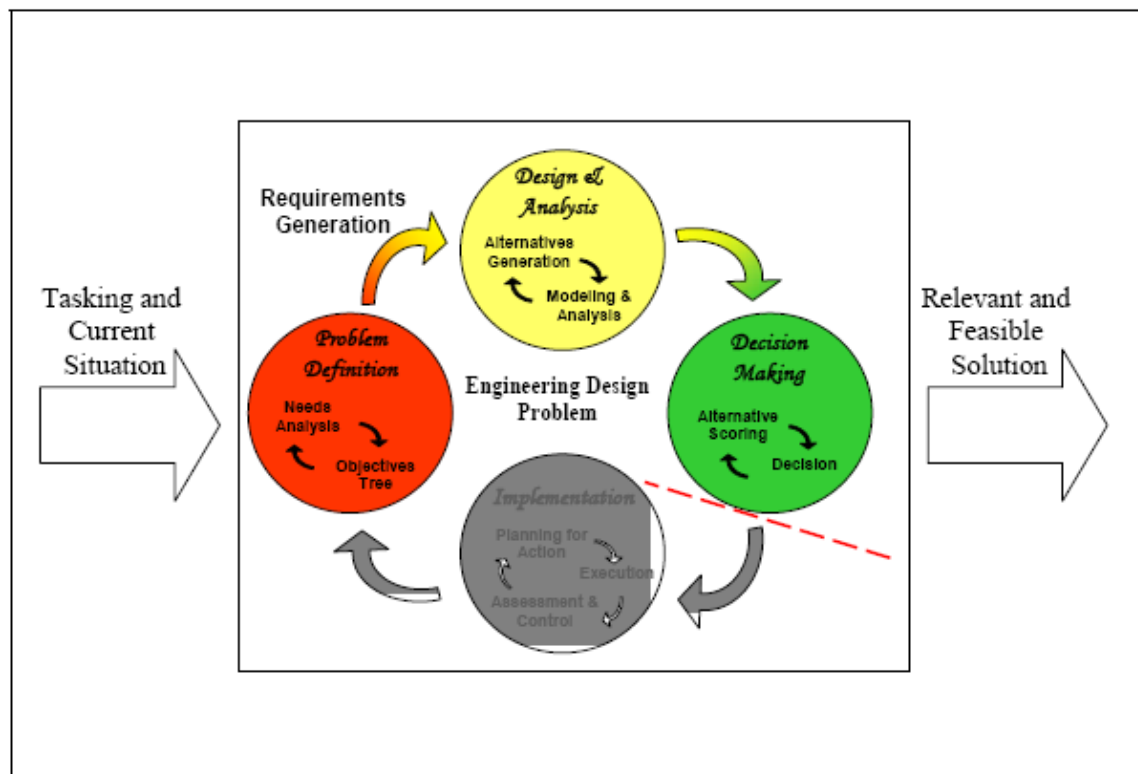
RADM (Ret) Richard Williams
Professor Gene Paulo
Professor Gary Langford
Professor David Olwell
Professor Francis Shoup
Professor Mark Stevens
CAPT (Ret) Thomas Hoivik
Professor Matthew Boensel
Professor Ronald Fricker
CDR David Schiffman
Professor Robert Harney
Professor Wayne Hughes
CAPT (Ret) Jeffrey Kline
Professor Daniel Nussbaum
Professor Bard Mansager
Professor Doyle Daughtry
Professor William Solitario
Professor Cristi Roberto
Professor Tummala Murali
Professor Don Brutzman
Professor Arnold Buss
Professor Gamani Karunasiri
Professor Richard Harkins
Professor Lyn Whitaker
Professor Susan Sanchez
Mr. Ed Hughlett
Mr. Michael Andrews

Additionally, we would like to thank our families throughout this endeavor - for their love, patience, understanding, and sacrifice over the past year and a half. Without their support, none of this would have been possible.

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The 2007 Naval Postgraduate School (NPS) Systems Engineering and Analysis (SEA) Integrated Project titled “Port Security Strategy 2012” (PSS12) was a joint product developed by eight NPS SEA students and 17 National University of Singapore (NUS) Temasek Defense Systems Institute (TDSI) students. The tasking letter from the Wayne E. Meyer Institute of Systems Engineering directed the Integrated Project to design a conceptual system of systems to improve port security measures for U.S. ports and force protection options for U.S. forces in U.S. and foreign ports. Port Security Strategy 2012 used the Systems Engineering Design Process as a tool to create a relevant and feasible solution given the tasking and on the situation postulated for the 2012 timeframe.



Systems Engineering Design Process

Following the September 11, 2001 terrorist attacks, the U.S. government shut down the air traffic system for two days and temporarily suspended the maritime

transportation system, preventing ships from entering U.S. ports. The United States realized that if a plane could be used as a feasible weapon, a ship and its cargo may also be used in a similar manner, shutting down a port and resulting in severe economic ramifications. For example in June 2002, an International Longshore and Warehouse Union strike ceased operations on all major U.S. West Coast ports. According to a Martin Associates study, a 10-day shutdown of the west coast ports cost the U.S. economy \$19.4 billion. If the shutdown had extended to 20 days, the economic impact was postulated to increase to \$48.6 billion dollars [1].

PSS12 involves a variety of stakeholders, each of whom holds different responsibilities. Their scopes of concerns were defined by local geography, economic, and political considerations, which led to four isolated but related areas of interest; consequently, PSS12 examined four areas concerning the range of issues raised by stakeholders. Organizations interested in port security include the Department of Homeland Security, United States Coast Guard, Marine Terminal Operators, Department of Defense, Regional & Local Police, Republic of Singapore Navy, Singapore Coast Guard, Singapore Civil Defence Force, among others. Each potential stakeholder presented different concerns, needs, and requirements, which were used to scope and bound the port security problem. Different stakeholders identified four primary areas of concern: threats originating from land (terrestrial threats), threats originating from foreign ports (source seaborne threats), threats originating from local waterways (regional seaborne threats), and threats originating from port employees (internal personnel threats). In order to address these primary areas in enough detail, it was essential to divide the team into four subgroups of five to six students each to address each issue.

Port Security 2012 formed the Terrestrial Threats Group (TTG), the Source Seaborne Threats Group (SSTG), the Regional Seaborne Threats Group (RSTG), and the Internal Personnel Threats Group (IPTG). The TTG considered threats from the land perimeter of the port to the pier-side ship. The scenario the TTG examined involved a container truck laden with explosives, which attempts to gain access to a terminal in a major U.S. port by speeding past security at the terminal's entrance. The SSTG considered threats arriving from overseas ports. The SSTG scenario involved terrorists

coordinating a flood of containers holding weapons of mass destruction onto cargo ships bound for a domestic U.S. port. The RSTG considered waterborne surface threats from within the port boundary to the pier-side ship. The RSTG scenario involved multiple small boat attacks against moored ships and port infrastructure. The IPTG considered threats from personnel, who may or may not be employed by the port facility. The scenario the IPTG examined involved personnel collaborating to create maximum port infrastructure destruction.

Using the Systems Engineering methodology, PSS12 defined the problem and created threat scenarios. Each team constructed alternative system of systems for each scenario considered. Performance for each alternative was modeled, analyzed, and compared using predetermined measures of performance and effectiveness. Implementation deadlines and constraints contributed to alternative risks. The system implementation must be feasible within five years.

Consensus amongst the stakeholders required minimal impact on the flow of commerce in a commercial port and the flow of operations in a military port. Each alternative examined will incur research and development, procurement, and operating and support costs. Performance based on the modeling metrics, risk based on the economic or operational impact, and cost based on the total system cost are determining factors among system alternatives.

A number of modeling tools (e.g. MANA, Arena, Extend, Simkit, and/or Excel) were used by the TTG, RSTG, SSTG, and IPTG to evaluate the measures of performance effectiveness for each alternative and the status quo. Data from these models were collected and analyzed to compare these alternatives against current systems. Cost data and measures of effectiveness were coupled to determine a system that provided adequate effectiveness for reasonable cost. The model results and analysis would enable the stakeholder to make a well-informed decision regarding the employment of future systems in port security.

The key findings of the four operational scenarios are described on the following page:

Terrestrial Threats Group

- The TTG considered a possible vehicle-borne IED attack on a port facility. Perimeter security requirements significantly differ amongst all ports. Geographic, social, and legal constraints directly influence the feasibility of employing certain systems. The most important step in defending against vehicle-borne IEDs is to harden the perimeter barriers by steel-reinforced concrete blocks to the base of the existing chain link fencing.
- With the perimeter barriers in place, the gate is the only alternative point of terrestrial entry for vehicle-borne IEDs. Based on the modeling results and the cost benefit analysis, additional armed guards should not be employed due to their marginal improvement in effectiveness at high cost. Either the spike strips or pop-up barriers alternatives should be employed. While pop-up barriers are twice as effective as spike strips, they are also twice the cost.

Regional Seaborne Threats Group

- The RSTG considered multiple small boat attacks on the Port of Oakland. The small boat attack consisted of the simultaneous attack of 1, 2, 3, 4, 5, 6, 9 or 12 boats. The RSTG deployed various sensors and platforms in an attempt to successfully interrogate potential contacts of interest in order to avert an attack. A successful interrogation required the contact of interest to be in the sensor's classification/recognition/identification range for three minutes of simulation time. The percentage of terrorist successfully interrogated was the primary MOE.
- Based solely on the cost benefit analysis, the RSTG found that the addition of an Unmanned Surface Vehicle and two additional X-band radar stations (located on southern Tiburon Peninsula and at the southwest point of the former Alameda NAS) provided the most effectiveness for the least cost in one half of the scenarios. The addition of Sonar to the defense package drastically increased cost with marginal benefit. In six of the eight cases examined, the addition of a single X-band radar yielded largest improvement in terrorist detection rate over cost.

Source Seaborne Threats Group

- The SSTG considered the importation of 12 dirty containers from foreign ports. Using a transshipment hub, where thousands of containers are handled daily, terrorists can potentially introduce containers containing contraband into the shipping network. Sensors are deployed at the port of entry, crane spreaders, and holding yards to detect the presence of dirty containers. Customs inspections team would further be utilized to intrusively inspect all flagged containers suspected of container weapons of mass destruction. The primary MOEs considered include the probability

of detection, false alarm, missed detection, productivity, and average time to inspect each container.

- The best alternative is the high performance alternative which employs the Automatic Targeting System+, a gamma scanner and HAZMAT detector at the container holding and loading areas, and a fully equipped inspection station. These alternatives results in a cost of \$82.67 million. A significant sensor mix is necessary for a high probability of detection. This sensor configuration should include a gamma scanner at the port of entry, radiation detectors and gamma scanners at holding areas, a scale and gamma scanner at loading areas, and a gamma scanner, HAZMAT detector, and trained animals at the intrusive inspection station.

Internal Personnel Threats Group

- The IPTG considered unauthorized employee physical access and unauthorized employee data access. Three models (Excel, Extend, and MANA) were used to determine the effectiveness of each alternative. The Extend and MANA models were integrated to produce the probability of interdiction for unauthorized physical access. Unauthorized data access was modeled using Excel.
- The current system has a 12 percent probability of interdiction for unauthorized physical access and 81 percent probability of interdiction for unauthorized data access. The presence of a mid-terminal fence with an open gate policy improved the probability of interdiction by 97 percent over the baseline. Combining communications, mid-terminal fence, and a triggered shut gate policy increased the probability of interdiction by 172 percent over the baseline.

While specific threats were examined by each of the respective groups, there remain other unexamined threats. The threats not examined in this report were not high priority threats as indicated by the PSS12 stakeholders. Some of these threats include air, mine, swimmer, underwater vehicle, and unmanned system threats.

Different agencies, whose efforts collectively provide port security, have different jurisdictions, organizational structures, and funding. A coordination problem exists amongst different agencies. The information received from the agencies must be rapidly received, displayed, interpreted and responded to in order for many of the modeled alternatives to be effective. From conducting this study, PSS12 recognized that the

fusion of data is a critical issue that needs to be addressed. Data fusion was beyond the scope of this project; however, is an area where future study is required.

Section I introduces the purpose of this study to include the background, concept of operations, operational environment, threat scenarios, scope, method, and chronology. Sections II, III, IV, and V introduce the needs analysis, alternatives generation, models, results, and analysis for the terrestrial threats group, regional seaborne threats group, source seaborne threats group, and internal personnel threats group, respectively. Section VI describes the conclusions, recommendations, and areas of future study for each of the subgroups.

I. INTRODUCTION

A. BACKGROUND

1. Port Security, Shipping, and Commerce

The Global presence of U.S. Navy and Commercial Ships has always presented lucrative terrorist targets. U.S. Navy and Commercial ships are the most vulnerable while pier-side. Incidents such as the USS Cole (DDG 67) bombing in 2000 and the USS Kearsarge (LHD 3) rocket propelled grenade (RPG) attack in 2005 confirmed that even the mightiest warships are vulnerable to terrorist attack while in-port. Another lesson learned from these incidents is effectively attacking an in-port ship does not require advanced tactics or hardware. The USS Cole was almost sunk by a slow, explosive laden surface vessel. The USS Kearsarge was missed by terrorists shooting RPGs from a rooftop in close vicinity to the port. Defending a pier-side ship presents many challenges. There are several avenues from which a terrorist threat may originate. If the threats are allowed port entry via water or land, protecting an in-port ship presents a difficult challenge. The identification and neutralization of terrorist threats before port infiltration will provide the best results. The task of protecting an in-port ship is best accomplished by defending the hosting port from potential terrorist threats or incursions, but measures to accomplish this might cause unacceptable impediments to port operations.

Commercial ports and naval bases are high profile terrorist targets. Commercial and Naval Ports are often located near major metropolitan areas with high population densities. A successful terrorist attack on one of these facilities could endanger the local populace. The geographic locations of the top ten U.S. Container ports are shown in Figure 1.

A successful terrorist attack on a maritime port causes enormous economic ramifications. The safe and efficient operations of Commercial Maritime Ports are critical to the world's economy. Over 60 percent of U.S. petroleum and 93 percent of all U.S. imports and exports are transferred through maritime ports [2]. A successful terrorist attack on a ship in a major port could disrupt commerce at other major commercial ports as emergency procedures and extra security measures are enacted. Each day that a major

U.S. port is not operational costs the United States' economy and average of one billion dollars [3]. The shipping industry directly provides for hundreds of thousands of domestic jobs vital to the United States Economy.



Figure 1. Locations of Major U.S. Container Ports

Major U.S. Container Ports are located near densely populated areas. In close proximity to the numbered ports are: 1 & 2. Los Angeles, 3. New York City, 4. Charleston, SC, 5. Savannah, GA, 6. Norfolk, VA, 7. Oakland, CA, 8. Houston, TX, 9. Tacoma, WA, 10. Seattle, WA.

2. National Directives

Security of Commercial and Naval Ports has been set as a national priority in Homeland Security Presidential Directive 13 (HSPD-13). The directive emphasizes that security in the Maritime Domain is a global issue. The directive states that securing only domestic ports is not sufficient when dealing with hazardous cargos which are transported from foreign ports. Security policies must actively involve these ports to

maintain safety in domestic ports. HSPD-13 directs the Department of Defense and the Department of Homeland Security to form and implement a National Strategy for Maritime Security. Furthermore, HSPD-13 states this strategy should prevent terrorist attack and criminal acts in the Maritime Domain, protect population centers and critical infrastructures, and enhance international relationships by promoting the integration of U.S. allies and international and private sector partners to advance common security interests [4].

Ports are vulnerable from many different aspects. These aspects include but are not limited to the terrestrial perimeter, maritime domain, hazardous cargo, and internal personnel. Port security cannot be accomplished by a single system that addresses each of these potential problems. The chosen security measures in these realms must all contribute to the overall goal of securing a port which will result in securing the in-port ships.

The National Strategy for Maritime Security directs the deployment of a layered security system. To meet this requirement, the cooperation of many government, non-government, and foreign agencies is essential. The National Strategy for Maritime Security addresses this need by stressing that international cooperation is critical for ensuring that lawful public and private activities in the maritime domain are protected from attack. It further states that trust and confidence among the U. S. and its allies must be increased [5].

B. PURPOSE

The purpose of this study was to serve as the Systems Engineering and Analysis Integrated Project for SEA Cohort 11 (SEA-11) and Temasek Defense Systems Institute (TDSI) of Singapore. The objectives of the Capstone Project are to provide educational content appropriate to future professional careers as senior leaders and apply course content to the execution of the project. The SEA Cohort 11 and TDSI addressed a problem that is relevant to the U.S. Navy and other government agencies. The tasking letter from the Wayne E. Meyer Institute of Systems Engineering, dated 6 December

2006, titled this study Port Security/Force Protection (PS/FP) and presented the following guidance:

Design a conceptual system of systems to improve Port Security measures for U.S. ports, and Force Protection options for U.S. forces in U.S. and foreign ports. Potential Focus Areas:

- Develop a system of systems to provide individual ship self protection for U.S. Navy combatants
- Develop concepts and systems for the integration of U.S. Navy shipboard self protection systems with U.S. Navy shore based systems.
- Develop concepts and systems for U.S. commercial port security systems and the integration of U.S. Navy combatants and commercial vessels into these systems.

The tasking letter provided the PSS12 team with initial guidance. Research dictated that a current primary concern in the maritime domain is in the security of ports, thus shifting the focus from force protection and port security of U.S. ports and U.S. forces to port security of U.S. commercial ports. This study was directed to remain fully Unclassified with the cooperation of the TDSI of Singapore. The initial guidance was provided in HSPD 13; “Maritime Security Policy”, National Strategy for Maritime Security, and National Plans for Maritime Security. Additionally, the study is to examine alternative technical solutions looking within a five year timeframe. This restricted the examined alternatives to those already at technical readiness level four (laboratory component validation) or higher.

Each group was designated to consider: 1) what is the biggest threat to in-port ships? and 2) how much of an impact on normal operations are tolerable to increase overall security.

C. CONCEPT OF OPERATIONS (CONOPS)

A CONOPS was established to resolve issues that surfaced while addressing the problem of port security. The SEA 11 PS/FP Team discussed different options on how this problem should be addressed. The SEA 11 PS/FP Team determined the best method to address the problem was to divide the problem into avenues from which threats could originate. The avenues were defined as:

- Terrestrial Threats
- Regional Seaborne Threats
- Source Seaborne Threats
- Internal Personnel Threats

In effect this approach defined four loosely integrated areas of concern which would each be analyzed using our systems engineering methodology. The team divided into groups consisting of five to six personnel to examine each avenue. Each group used the SEDP to define their problem, design alternatives, model the alternatives, analyze the data, and report the results.

The terrestrial threats group (TTG) examined the threats that originate from the landward perimeter of the port. These threats included vehicle borne improvised explosive devices (IEDs) or unauthorized personnel entering the port perimeter. The TTG examined and modeled alternatives to detect and engage the possible threats. The goal of these systems was to protect port assets from threats that originate from land.

The regional seaborne threats group (RSTG) examined the threats that originate from the seaward side of an in-port ship to the port boundary. Possible threats from this realm include explosive laden boats, seaborne RPGs, mines, swimmers, and hijacked commercial vessels. The RSTG also examined and modeled alternatives to deter, detect, track and engage threats from this realm. The goal of such systems was to protect port assets including in-port ships from threats in the local maritime environment.

The source seaborne threats group (SSTG) studied the threats that could rise from the originating ports of arriving ships. Threats from these ports include the smuggling of illegal personnel, weapons of mass destruction, or sabotaging volatile cargo. The SSTG examined measures that could be implemented in source ports to reduce the hazards associated with arriving ships and their cargo. The goal of the system is to reduce the probability of these personnel and weapons threats from entering a port on an inbound ship.

The internal personnel threat group (IPTG) considered the threats that originate from personnel who may or may not be employed in the port facility. Threats include but are not limited to internal security breaches by employed personnel or security breaches

into the port and ships by personnel who are not employed at the facility. The IPTG studied measures to reduce the in-house threat presented to the facility.

D. OPERATIONAL ENVIRONMENT

The Port of Oakland and Port of Singapore were the primary stakeholders for PSS12. The close proximity of the Port of Oakland allowed easy access to port facilities and personnel. The TDSI students from Singapore had points of contact for personnel at the Port of Singapore to aid the PSS12 research. Each of the groups analyzed the operational environment for the Port of Oakland and Port of Singapore.

1. Terrestrial Threats Group (TTG)

a. Boundaries of the Area of Operation

The boundaries of the area of operations for both the Port of Oakland and the PSA Singapore Terminals (PSA) are defined as the area from the waterside to port inland boundaries which are demarcated by perimeter fences. At both ports, the geographical boundaries are well defined.

In the Port of Oakland, there are a total of 11 terminals, and adjacent terminals are separated by 8 ft wire mesh fences with barbed wire outriggers. A different port operator operates the individual terminals. The security of the individual terminals is the responsibility of the respective port operators. The Oakland Railport will not be included in the study as they are not under the purview of the port operators. The Oakland Railport includes the Burlington Northern Santa Fe Intermodal Yard and the Union Pacific Intermodal Yard as shown in Figure 2.



Figure 2. Terminals at the Port of Oakland

PSA has a total of four container terminals and two multi-purpose terminals. The security of the terminals is also the responsibility of PSA. The physical layout of the Port of Singapore is depicted in Figure 3.



Figure 3. Terminals at PSA Singapore

Following the completion of the Pasir Panjang Container Terminal, there will be 45 container berths. Twenty-three multi-purpose berths are located within the two terminals.

b. Size of Area of Operations

Both ports contain large geographical areas that the terminal/port operators are responsible for securing. At the Port of Oakland, the size of the entire port

is approximately the area of 590 football fields, while the combined area of all PSA terminals is approximately 790 football fields. The ports have long length wharfs that are easily accessible from the open harbor channels. Table 1 summarizes and compares the physical size of the Port of Oakland and Port of Singapore.

	Port of Oakland [6]	Port of Singapore [7]
Total Terminal Area	~ 318 hectares	~ 423 hectares
Total Number of Berths	20	45
Total Berth Length	~ 6 km	~ 13 km

Table 1. Physical Port Size for Port of Singapore and Oakland

The physical dimensions of both the Port of Oakland and the Port of Singapore are large. Each hectare is equivalent to an area of 10,000 square meters or 107,639 square feet. While the Port of Singapore is only 1.33 times larger than the Port of Oakland, the Port of Singapore houses more than twice the number of berths and exceeds twice the length.

c. Port Topology and Characteristics

The entire terrain of both ports is flat in order to better facilitate the movement of containers. However, containers are usually stacked vertically for storage, sometimes up to four containers high (4m x 2.59m). The stacks of containers present challenges for ground surveillance as they obscure lines of sight.

The Port of Oakland is served by a variety of transportation networks that include freeways, public roads, service roads and railroads. Major transportation networks at the Port of Oakland include:

- Freeways: I-80 Northbound & Eastbound, I-880 Southbound, I-580 Eastbound, I-980 Eastbound
- Railroads: Burlington Northern Santa Fe, Union Pacific
- Bridges: San Francisco Bay Bridge
- Landing Beach and Sites: All Wharfs, Middle Harbor Shoreline Park

The San Francisco Bay Bridge located north of the Port of Oakland provides a visual vantage point for the wharf fronting the Oakland Outer Harbor Channel.

The Port of Singapore is served by a network of expressways, public roads and service roads within the port area. However, it is not served by any railroads or bridges. Possible landing sites for vessels from the harbor channel include all wharfs on the Port of Singapore waterfront.

Defensive barriers are critical in securing critical port infrastructures. Perimeter fences and guard gates are some of the capabilities that the Port of Singapore and the Port of Oakland employ. Physical defensive measures in use by both Port of Oakland and PSA to deter unauthorized intrusion are shown in Table 2.

	Port of Oakland	Port of Singapore
Perimeter Fences	<ul style="list-style-type: none"> • 8 ft single layer wire mesh fences with barbed wire outriggers 	<ul style="list-style-type: none"> • 3 m wire mesh fence
Guarded Gates	<ul style="list-style-type: none"> • Entry points guarded by unarmed security personnel throughout day • Gate arms employed to control traffic flow at selected gates • No physical obstacles (concrete barricades, pop-up barriers) to force incoming vehicles to slow down. 	<ul style="list-style-type: none"> • Employ “pop-up” barriers to block or puncture vehicle tires to slow down forced vehicular entry

Table 2. Defensive Barrier Employment

The Port of Oakland has significant disadvantages in physical security compared to the Port of Singapore. While the Port of Singapore employs pop-up barriers, no physical barriers at the Port of Oakland can adequately slow down traffic.

The key terrestrial features that surround the Port of Oakland include the Middle Harbor Park at the Port of Oakland. This territory is considered a public access

area. A public park in the midst of the terminals means that the entire port area could not be totally restricted to better control accessibility. The park is bounded by the Trapac Terminal (Berths 30 to 33), the Evergreen Terminal (Berth 34), the Ben E. Nutter Terminal (Berths 35 to 38), the Hanjin Terminal (Berths 55 to 56), and the Burlington Northern Santa Fe Intermodal Yard on the west side. The Port of Oakland also houses the Alameda-Oakland San Francisco Ferry Terminal with close proximity to the Charles P. Howard Terminal (Berths 67 to 68).

Critical infrastructures located in and around a port can stop or slow down port operations. At the Port of Oakland, the power substations and computer network servers, located within the port area, maintain continued port operations. Telephone poles along roads, protected by small mesh fencing and bollards, constitute the lines of communication between terminals, authorities, and other outside agencies and organization. Similar to the Port of Oakland, power substations and computer network servers are two readily identifiable PSA critical infrastructures.

2. Regional Seaborne Threats Group (RSTG)

a. Port of Oakland

The Port of Oakland is one of the United States' busiest container ports on the West Coast because of the renovation to the berths, installation of new container cranes, and the deep water channels. Oakland is the container port gateway for the fourth largest U.S urban market, serving more than seven million people. The Port of Oakland, which encompasses 759.3 acres, is not owned by one corporation but multiple corporations where business is exporting and importing commerce to the U.S. and other countries. With the increase of vessel traffic, the need to maintain productivity while insuring security of the merchandise is of extreme importance. Through the process of running security drills and scenarios, as well as working with the Department of Homeland Security (DHS), in particular United States Coast Guard (USCG), the Port of Oakland believes its security is acceptable. As the assets of DHS are occupied with more critical and time sensitive issues, the role of protecting the ports of commerce will fall by the wayside. Therefore, there is a gap in the port security aspect pertaining to the

waterside access to the pier as well as to ships tied to the pier. Port of Oakland provides waterway access throughout the Oakland metropolitan area for the recreational sailors to motorboat operators. In the United States, the limit to infringe upon the rights of free passage of the waterways for the pleasure crafts is difficult to enforce and maintain. From this aspect alone, the port is a soft target for those wishing to cause damage.

b. Port of Singapore

Situated at the maritime crossroads between the East and West, Singapore has been the world busiest port since 1986 in quantity of shipping tonnage. Singapore is the focal point of some 200 shipping lines with links to more than 600 ports in 120 countries. More than 50,000 ships pass through the straits of Malacca and Singapore annually, carrying half of the world's oil and almost one-third of the world's trade [8].

The maritime trade plays a crucial role in the development of Singapore's economy. Since its independence, Singapore's continued prosperity and development hinges greatly on the security of the straits and ports. Singapore's strategic location, coupled with her excellent physical infrastructure and stable government, enables this country to be an effective shipping hub and capitalize on the shipping trade by providing the necessary services to passing ships.

Singapore is one of the world's busiest container ports having handled 24.8 million TEUs (Twenty-Foot Equivalent Units) of containers in 2006. As the world's busiest seaport and largest transshipment hub, the port of Singapore attracted approximately 140,000 vessel calls. At any one time, there are some 1,000 sea-going vessels operating within Singapore's waters [8]. Singapore also received approximately 50,000 calls by regional ferries and cruise vessels.

Singapore is the third largest oil refining center in the world with major oil companies such as Shell, ExxonMobil, Chevron, and Texaco operating at Jurong Island. More than 12,000 oil tankers and 3,000 chemical tankers call at Singapore a year. With the rapid and continuing development of Jurong Island into a major petrochemical hub, an increase in the number of tanker calls can be expected [8].

There are a total of thirty-two anchorages and forty-one container berths along seven and one half miles of quay length in the port infrastructure. The anchorages are designated to serve specific purpose for different types of vessels, depending on the type of vessels and the type of goods the vessel is carrying. An example is shown in Table 3 on the following page. The port infrastructure is situated along the southern coast of the island [9].

The Port of Singapore is comprised of four container terminals and two multi-purpose terminals. Following the completion of the Pasir Panjang Container Terminal, there will be 45 container berths. Twenty-three multi-purpose berths are located within the two terminals.

Singapore maritime territorial sea claim is three nautical miles from its coastal line [10]. The transit waterway is in between islands belonging to Singapore and Indonesia.

The Maritime and Port Authority of Singapore (MPA) is the statutory board which regulates and licenses port and marine services and facilities for port of Singapore. It also manages vessel traffic in the Singapore port, ensures navigational safety and port/maritime security, and a clean marine environment [11].

PSA Singapore Terminals is presently the port operator for port of Singapore. In addition to Singapore's throughput, it handles about one-fifth of the world's total container transshipment throughput and 6% of global container throughput [12].

Anchorage	No.	Purpose	Location
General Purposes	1	Vessels requiring immigration clearance and bound for shipyards and facilities in the East Johor Strait and vessel's using the scheme for taking ship's supplies and/or changing crew.	Eastern
Holding	1	For general purposes with prior permission of the Port Master and for vessels under the scheme for taking ship's supplies and/or changing crew.	Eastern
Man-of-War	1	For visiting warships.	Eastern
Special Purpose (A)	2	For vessels with prior permission of the Port Master and vessels taking bunkers using the Special Bunkering Anchorage Scheme.	Eastern
Special Purpose (B)	2	For vessels under arrest, damaged vessels, vessels requiring repairs and other vessels with prior permission of the Port Master.	Eastern
Petroleum	2	For vessels loaded with petroleum and non-gas free vessels.	Eastern
Special Purpose (C.)		For vessels under arrest, damaged vessels, deep draught vessels, vessels requiring repairs and other vessels with prior permission of the Port Master.	Eastern
Laid-up Vessels	1	For vessels laid-up in port.	Eastern
Small Craft	1	For harbour tugs, pontoons, barges and other small craft, include fishing vessels.	Eastern
Explosives Lighters	1	For small craft loaded with explosives.	Eastern
Eastern	1	For general purposes such as receiving stores, water, bunkers, waiting for berth by vessels other than non-gas free petroleum carriers, liquefied natural gas carriers, liquefied petroleum gas carriers and chemical carriers.	Eastern
Holding (A, B)	2	For vessels as directed by the Port Master.	Eastern
Holding (C.)	1	For port limit tankers that are waiting to service vessels in Keppel Harbour.	Eastern
Barge Temporary Holding	1	For barges loaded with sand/granite waiting to proceed to an approved aggregate terminal in the East Johor Strait or as directed by the Port Master.	Eastern

Table 3. Eastern Sector Anchorages Examples

The examples of Eastern Sector Anchorages indicate special locations for temporary barges, warships, explosive lighters, small craft, petroleum, and general purpose vessels.

c. Naval Assets

In the case of a Navy ship, the ship and its crew are not as helpless as that of a containership. There are a lot more assets available at the Commanding Officer's (CO) disposal to protect and defend his ship. More avenues are given to a ship that is underway rather than pierside. It is during the moored time when a naval ship is at high risk to terrorist attack. When a naval ship is moored in its homeport, such as: Norfolk, San Diego, Mayport, and Pearl Harbor, the chance of a terrorist attack is reduced because of Naval Installations Command providing port security and force protection measures needed, but the threat still exists. It is up to the CO, as well as the crew to protect the ship when it is in port. A naval vessel is most vulnerable when it is in a foreign port implementing its own force protection measures. When an issue arises for a naval ship in a foreign port, a vital question is should it employ lethal or non-lethal force. Besides standing watches that provide 360 degree coverage of the area around the ship, there are also random measures placed to keep the activities onboard a naval ship variable and not repetitive. To help with the operational environment, the concept of the imaginary boundary is created around the ship to provide time to react to the threat in a timely effective manner. Even though the naval ship has means at their disposal to react to a waterside threat, the threat remains similar to that of commercial ships.

3. Source Seaborne Threats Group (SSTG)

The area of operations considered by the SSTG includes the PSA and the open ocean transit waters to the waterside boundary of the Port of Oakland. In 2006, PSA processed 23.98 million twenty-foot equivalent units (TEUs). PSA operates the four major container terminals in Singapore: Brani Terminal, Kepple Terminal, Pasir Panjang Terminal and Tanjong Pagar Terminal. These four terminals have a combined area of 1077 acres containing 28 main and 16 feeder berths. These terminals also enclose the world's largest refrigerated container (reefer) facilities with approximately 4900 reefer points and servicing more than 500,000 reefers in 2006. Figure 4 shows the location of the Tanjong Pagar Terminal and Brani Terminal located in the southern region of Singapore. Each of these terminals operates 38 quay cranes and 165 yard cranes to handle stevedore services at the pier and to manage container storage facilities at the yard.



Figure 4. Tanjong Pagar and Brani Terminals

The Tanjong Pagar Terminal and Brani Terminal operate 38 quay cranes to provide stevedore services and 165 yard cranes to manage the transshipment containers.

The total area of the open ocean transit environment comprises 165.384 million square kilometers, 18 times the size of the continental United States and larger than the Earth's land area. The major shipping lanes that may be involved with a shipment from Singapore to Oakland are the trans-Pacific, Far East Europe, intra-Asia, South-East Asia and Australasian lanes [13]. The various shipping lanes centered on Singapore are displayed in Figure 5.



Figure 5. Shipping Lanes of Asia

4. Internal Personnel Threats Group (IPTG)

The workers at the Port of Oakland are divided into four major categories: longshoremen, clerks, foremen, and watchmen. The longshoremen are mainly the workers loading and unloading the containers. They are the main bulk of the workers at the port, and there are about 1800 longshoremen employed in the Port of Oakland. The clerks are mainly the administrative workers tracking the cargo movement. There are about 100 clerks employed in the Port of Oakland. The foremen are the supervisors of the workers, and there are approximately 40 foremen employed at the Port of Oakland. The watchmen are responsible for carrying out the security measures to monitor and report any discrepancies. There are approximately 60 watchmen in the Port of Oakland.

Screening at the Port of Oakland is accomplished by the National Vessel Movement Center (NVMC) and the Customs Border Protection (CBP). The NVMC is an intelligence coordination center that is part of the United States Coast Guard. It extensively screens passengers, crew and cargo based on the information provided by the ships. However, this only applies to all ships over 300 gross tons, and the information

must be provided 96 hours before arrival. In addition to the NVMC, the CBP plays a vital role in ensuring port security. Shipping companies are required to provide a cargo manifest at least 24 hours before the cargo containers arrived in the United States. This data is used by CBP's National Targeting Center to identify high risk cargo. The CBP uses a risk based analysis and intelligence to pre-screen, assess and examine 100% of suspicious containers. The remaining cargo is cleared for entry using advanced inspection technology. The CBP also work with foreign customs authorities to examine all U.S.-bound high risk cargo while they are still at foreign port.

The Maritime Transportation Security Act, 2002 (MTSA) documented two key pieces of legislation that play a role in port internal threats: prohibition and issuance of identification cards.

Prohibition. “ The Secretary shall prescribe regulations to prevent an individual from entering an area of a vessel or facility that is designated as a secure area by the Secretary for purpose of a security plan for the vessel or facility... unless the individual holds a transportation security card ...or is accompanied by another individual who holds a transportation security card..”

Issuance of cards. “ The Secretary shall issue a biometric transportation security card to an individual... unless the Secretary decides that the individual poses a security risk.. warranting denial of the card.

The Transportation Worker Identification Credential (TWIC) is a biometric card that has digital photograph, fingerprints and pin of the worker. It has multiple level of authentication through possession of card, photographs, fingerprints and pin verification. Every employee of the port will be required to have a TWIC. These include port facility employees, vessel operators, truck drivers, contractors, maintenance personnel, longshoremen, train crews and other dock workers. It is expected to be implemented in all ports by 1 January 2009. Currently, the TWIC reader requirement is withdrawn and the card reader technology is in development.

E. THREATS AND THREAT SCENARIOS

1. Terrestrial Threats Group

Threats of the land component can be defined as elements that support actions intended to disrupt the operation of the port or use the port as a means to facilitate the unauthorized importation of WMDs or terrorist cells. The disruption of port operations may come in three forms:

- Injuring and/or evacuation of port workers
- Damaging infrastructure of the port
- Contaminating port facilities with a chemical weapon or a dirty bomb

Vehicle-borne IEDs and pier-side release or detonation of weapons of mass destruction (WMD) have been identified to be the prominent land threats to port operations.

Vehicle borne IEDs are improvised explosive devices carried either in a vehicle or inside a shipping container. IEDs can be made easily from readily available materials. The delivery of such devices is noted to be either by personnel (suicide bombers) or vehicles. From the various IED bombing incidents on 1 October 2005 in Bali, Indonesia, on 9 September 2004 at the Australia Embassy in Indonesia, on 5 August 2003 at the Marriott Hotel in Indonesia, and on 19 April 1995 in Oklahoma City in the United States, it was noted that vehicle borne IEDs are preferred mode of terrorist operation as it has enough explosive power to cause significant damage to infrastructure which, in the case of a port, may severely impact port operation.

WMDs are weapons that possess the capacity to inflict extensive damage to infrastructure or the populace, or deny the use of critical geography through contamination. The successful deployment of a weapon of mass destruction would result in large economic loss and/or loss of life. A detection or activation of a WMD in the port would result in the disruption all port operations. Importation of a WMD provides terrorists the ability to inflict severe damage in the importing country. Weapons of mass destruction are classified as:

- Fissionable or fusionable nuclear weapons
- Chemical weapons
- Biological weapons
- Non fissionable or fusionable radiological weapons (dirty bombs)

Containers provide terrorist a method to gain unauthorized access into a country. It is possible for terrorist to infiltrate a shipping container in the container's country of origin and travel inside the container to its destination with WMDs. If the terrorists are not detected, they will have unauthorized access to the importing nation, enabling them to execute malicious intentions.

The possible security threat scenarios from the land component were classified into two categories: Minor threat scenarios and Major threats scenarios. Minor threats are defined as those when executed, will not have significant economic impact on the economy. It is suggested that any land security threats that result in the disruption of port operations for one terminal is classified as a minor threat. Major threats, on the other hand, are defined as threats when executed, will result in significant economic impact. It is suggested that the disruption of more than one terminal be classified as a major threat. Major threats include the unintentional importation of WMDs and terrorist operatives.

a. Minor Threat Scenarios

The first scenario considered was a minor threat scenario that involved localized damage to non-critical port infrastructures by forceful vehicle entry with an IED. A truck loaded with an IED either penetrates the eight-foot perimeter fence with barbed wire outriggers or refuses to stop at a gate and detonates at non-critical infrastructure. While this would likely result in minor economic losses and possibly some loss of life, the majority of the port would likely remain operational.

b. Major Threat Scenarios

The second scenario considered localized damage to power sub-stations, fuel storage/distribution location, or passenger cruise ship terminal by forceful by a vehicle-borne IED. The non redundant power supply to the port's cranes is located within the premises of the port, but only protected by small mesh fencing and bollards. It is

possible for a vehicle carrying an IED to penetrate the port's perimeter fencing, or refuse to stop at the gate, and proceed to drive through the fencing protecting a power substation and detonate the IED. This action would result in damaging the power substation which disrupts the power supplied to a substantial portion of the port's cranes. If the ports' cranes lost power, the port would lose ship on-load and off-load capabilities. This action would halt port operations in the affected portions of the port until the power substation could be repaired. An attack on a fuel storage location would likely cause severe pollution. If a terrorist was able to attack a cruise ship, they would likely kill several people, and decimate the cruise industry by inducing fear in its customers.

Localized damage to power sub-stations can also occur if a vehicle carrying an IED successfully penetrates the security gate. This third scenario considers a vehicle that obtains access to the port by driving through the gate with an undetected IED. The driver will then proceed to detonate his IED near a power substation and disrupt the power supply to the port's cranes.

Scenario four considered the successful importation of WMDs. Weapons of mass destruction in a container is imported and offloaded from a container ship, loaded onto a truck, and driven off the port facility without detection. This WMD (nuclear, radiological (dirty bomb), biological, or chemical) can be used to inflict severe damage on the importing nation.

Scenario five considered the successful detonation of WMDs in an imported container. Containers are scanned for radiological contents before leaving the port. It is possible for terrorists to detonate either a nuclear weapon or a dirty bomb in the port facility before the container is scanned. This action would result in the destruction or severe contamination of a substantial portion of the port. This would render the port unoperational for a substantial period of time.

Scenario six considered the successful importation of a terrorist cell. A terrorist cell is able to infiltrate a cargo container at the container's source port and is unintentionally imported to the destination country. They are not detected at the port and gain unauthorized access to the importing nation.

2. Regional Seaborne Threats Group

The team had identified the following threats as possible aggressive actions which will have a high severity and hinder the operations of the ports. The threats are as follows:

- Small boat attack on the port
- Large ship attack on the port
- Sabotage from swimmers
- Remotely launched projectile

The first scenario considered small boat attacks on ports. Small boats loaded with explosives can penetrate the waterside of the port and detonate in the port vicinity. This action would cause damage to the ports' systems and equipment and disrupt the normal operations of the port. From the military point of view, a small boat attack would elevate the force protection level of the ship. It would also create psychological effects within the U.S. populace and generate retaliatory outcries. The USS COLE (DDG 67) attack in Yemen in October 2000 and French tanker Limburg's attack in October 2002 demonstrated the potential major threat from the explosive-laden boats.

The second scenario considered was a large ship attack on ports. Ships laden with WMDs pose a potential threat. Another aspect to study is the use of the ship itself. Because of their large size and weight, the use of the ship as a kinetic weapon to port operations or to the military installations is a very viable threat. The large amount of momentum created by the large ship enables the infliction of severe damage to any vessel. If the large ship is laden with volatile cargo, the ship presents a major concern for port operations. Explosives from the ship can cause severe damage to the port, severely disrupting normal port operations.

Sabotage from swimmers was the third scenario considered. For example, the Straits of Singapore is narrow and busy and infiltrations may be launched from the neighboring secluded islands or small boats. The intent of the infiltration is to sabotage the key installations of the port by denying the operations of the port or by targeting high value contents in the containers. This is a minor threat that is applicable to ports that have islands in the vicinity of the port.

The fourth scenario considered remotely launched projectiles. Terrorists can launch missiles from boats in the harbors, straits or from neighboring islands. Portable projectiles can travel across the straits or be launched from a considerable distance from the port. These projectiles (i.e. RPGs) are equipped with high explosive warheads that may severely damage installations and port infrastructure. This is a moderate threat with more of a physiological and political effect rather than an economic effect.

The impact of the damage caused by the above threats has the potential to affect operations for extended periods of time.

3. Source Seaborne Threats

Threats are classified as elements whose purpose is to disrupt the activity of container ships or military operations within a port. The objective is to inflict damage to key infrastructure within the port and deliver undesired cargo into the U.S. that could be used in the execution of terrorist plots. Undesired cargo is categorized as:

- Human Operatives and Aliens
- Biological Agents
- Chemical Agents
- Radiological Material
- Explosives
- Drugs
- Smuggled Contraband
- Conventional Weapons
- Weapon Systems Parts

The SSTG identified four possible threats that may originate from the source port or in-transit between the source and destination ports.

- The smuggling of WMDs and other undesired cargo into United States.
- The infiltration of terrorists into the ship's crew and use of the ship as a kinetic weapon inside a U.S. domestic port.
- The sinking of a large vessel in restricted navigation waters disrupting shipping traffic into a port.
- The use of an aerial vehicle to contaminate merchant ships with explosives, radiological, biological and chemical materials for delivery or detonation within a port.

Several studies have examined the use of container ships to deliver undesired cargo to a United States seaport [14]. Explosives may be detonated upon container ship

arrival or after transportation to a high-value installation within the United States. Detecting undesired cargo, especially biological and chemical agents, inside a container presents technical challenges. Coupled with the vast amount of containers arriving at domestic ports, the task of detecting WMD and other undesired cargo is difficult. In most cases, sensors need to be placed in close proximity to the container to be effective. Scanning every container is time consuming and delays container shipment. In addition, cargo containers en route to the United States from overseas ports are not subjected to a consistent, rigorous inspection system. The inconsistent inspection system of these containers creates gaps in security where WMD and even terrorist operatives could enter the United States. If the WMD is missed during the subsequent security check conducted in the United States, terrorists could use these WMDs to wreak nationwide havoc. The SSTG proposes introducing additional security layers at the source port to prevent WMDs from being loaded onto container ships.

Terrorists also have the tactical advantage of timing which enables them to strike unexpectedly at various locations. They may infiltrate a ship's crew by progressing through the ranks and eventually attaining a key position. The infiltration option provides opportunities for the terrorists to seize control of the container ship and using the ship as a kinetic weapon against other shipping and port infrastructure. The examination of this scenario would involve looking at the possibility of continuous background checks to disrupt the terrorists' ability to infiltrate the commercial shipping industry.

The sinking of a large vessel in a strategic chokepoint can disrupt normal water traffic flow for extended periods of time. At the Port of Oakland, the width of the main estuary is slightly less than 150 yards, which is approximately the width of two container ships. The estuary has been dredged to 50 feet. The channel could be easily obstructed by sinking a large container ship in the center of the channel. Other than the financial loss associated with disrupted port operations, the impact of such an act would affect the military sealift capability as the Port of Oakland is designed for military use during national crises.

The technological advancement of Unmanned Aerial Vehicles (UAVs) makes them more difficult to detect. One UAV could be used to conduct an attack on merchant

vessels. With increasing payloads and range, UAVs could be launched from land sites or afloat platforms over the horizon to deliver their payload onto the transiting container ship. The payload could consist of radiological materials, explosives, and a remote detonator. Under the camouflage of darkness, UAVs can fly over the container ship undetected and drop the payload in the cavity created by the rows of containers. The potential bomb dropped would remain hidden among the containers until the ship arrives at the domestic port. An accomplice could remotely detonate the bomb while the ship is berthed.

Given the four primary threats considered by the SSTG, three different scenarios were hypothesized below.

Scenario One

Consistent oversight and enforcement compliance driven by the same inspection standards for every source port is impossible due to laws, politics, and regulations. Focusing on the largest transit port, Singapore, narrows the scope. A thorough system in Singapore, the busiest port in the world, would search the majority of the cargo and provide an additional layer of security for the destination port. The scenario involves WMDs being loaded onto a vessel in Rangoon, Myanmar and transiting through PSA. The WMDs are reloaded onto another container ship bound for the United States.

Scenario Two

Members of a terrorist cell have trained for several years as ship's crew. They have worked for several ocean carriers in a variety of jobs ranging from riggers to a ship captain. The terrorist cell has been activated and reports to work onboard a container ship, whose destination is the United States. Approximately half of the ship's crew is associated with the terrorist cell. The terrorists would seize control of the vessel while underway. The ship could rendezvous with a vessel laden with explosives and chemical agents, which are transferred to the ship. At the U.S. port, the ship could be detonated with explosives and sunk in restricted navigation waters, causing shipping traffic disruption and hindering port operations.

Scenario Three

Terrorists load weapons onboard a container ship in transit from Singapore to Oakland. Abu Sayyaf, an active terrorist organization, prepares at Mindanao for UAV operations. The UAV has either biological agents or explosives as its payload. The terrorists launch the UAV under the cover of darkness and fly it over the container ship identified by spotter vessels or aircraft. The biological agents and explosives are then dropped onto the container ship. At the Port of Oakland, the hazardous payload could be remotely detonated.

4. Port Internal Threats Group

Despite the security measures at the Port of Oakland, Mathew Gaines managed to bypass these measures and stowaway on two occasions. In the first incident, he was caught after a security watchman noticed Mathew Gaines in a maintenance uniform walking along a U.S. maritime vessel. Because no employee was scheduled to work that day, he was caught. In the second incident two months later, he was caught after setting sail across the Pacific to Japan and Taiwan.

Mathew Gaines' mode of operation was deceptively simple as he infiltrated security measures by stealing a jumpsuit, coat, radio and hard hat and disguising himself as a dock worker. Once aboard the vessels, he hid amongst the containers. Clearly implemented control measures were inadequate and need to be reviewed to prevent future occurrences.

Currently, all containers that come into the United States from foreign ports are screened using a manifest. The current inspection system relies on a computer which analyzes certain criteria of the shipment before determining the level of risk and requirement for inspection. With the illegal trafficking trade estimated at hundreds of billions of dollars, information that helps traffickers avoid inspection of illegal goods coming into the ports is extremely valuable. There are four classes of threats to a port.

- Organization that looks upon illegal act as a weapon to reach their goal. Eg. Terrorist cell. This is the most potent form of threat as their actions may lead to loss of infrastructure, income and impedance to the free flow of trade and goods.

- Organized Crime. Eg. Drug traffickers. This threat is possibly most likely but difficult to guard against as it would likely involve inside personnel working in the port.
- Single person on a mission who has the necessary knowledge and resource to cause problems. This form of threat is less likely but is potentially dangerous as this person is motivated by revenge, race, or religion.
- Small time criminal. Eg. Thieves. It is the most likely form of threat during day to day operation but it is likely to have the least impact on the Port.

The first scenario considers an individual or group with the purpose to cause maximum destruction to the port facility and the in-port ship. One way to achieve this goal is to break up the explosive weapons into various parts carried by different shipments into the port. The insider would coordinate the different shipment of weapons by selecting a shipment that is less likely to be marked for inspection. It is difficult to detect any possible existence of weapons since most components can be mixed with other legitimate items such as electronics, machinery and raw manufacturing materials. Alternatively, the random check conducted can also be exploited. Assembly of the weapons would be done by the insider(s) disguised as workers of the port (e.g. machinery operators, dock workers etc). Detonation of explosives would be coordinated in conjunction with the docking of a ship. The explosives could be installed near the bay and cargo landing areas (near to the fuel tanks of the ship). The attack potentially could generate enough fuel explosives to cause substantial destruction to the port.

The second scenario considers the targeting of critical information with respect to shipping schedules and detailed inspection plans. A group of workers currently employed by the port of Oakland have recently become more disgruntled by America's attack on Muslim societies in the Middle East. Over a period of several months, they have been in contact with some members of their local mosque. They have been asked to help obtain access to shipping information. The purpose is to order the ship to smuggle goods into the U.S. to help fund organizations and their plans to "liberate" their fellow believers from the U.S. oppression overseas. In order to do this, shipping logs and patterns from Afghanistan and nearby neighbors are required. They would like to export the every growing supply of opium grown in the fringes of Afghanistan to the United States. This accomplishes 2 things: Money for the "war" and also, further deteriorates the moral

fabric of the United States. They hope that by finding regular shipments and information about cargo inspections that they can more easily hide their shipments and circumvent inspection.

D. SCOPE

1. Participants

Port Security Strategy 2012 (PSS12) consisted of eight students from the resident NPS Systems Engineering and Analysis Program (NPS Curriculum #308) in addition to 17 students from National University of Singapore's TDSI program. The members of the group hailed from various backgrounds to include seven U.S. Navy, three Singapore Navy, two Singapore Air Force, one Northrop Grumman, two Singapore Technologies Engineering, one DSO National Laboratories, and eight Singapore Defense Science and Technology Agency representatives.

In addition to direct contributors to the research, the SEA-11 and TDSI students consulted students, staff, and faculty from other NPS departments and curricula, the Department of Defense, the Department of Homeland Security, the Port of Oakland, and the Port of Singapore to obtain relevant research related to the field of port security and force protection. A summary of the primary participants involved in this study is shown in Figure 6.

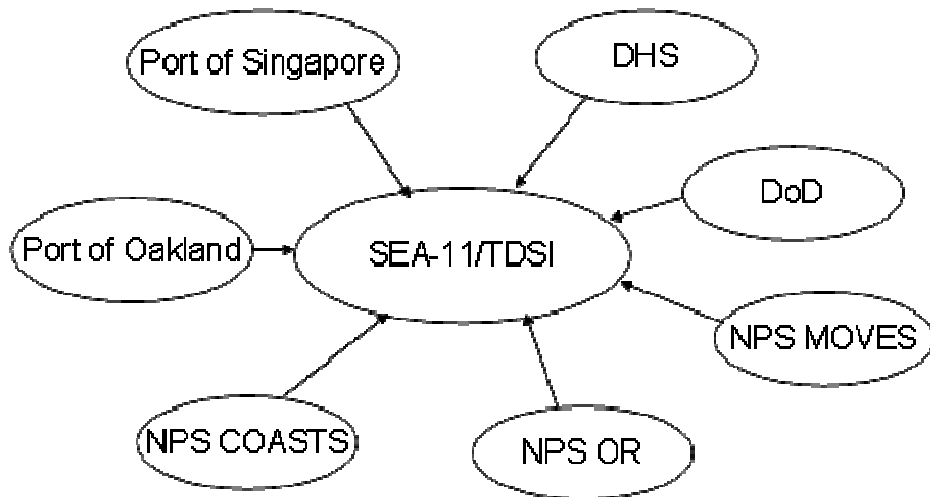


Figure 6. Integrated Project Participants

The SEA-11 port security and force protection project is fully integrated with various cross-campus departments, nearby and overseas ports, the Department of Defense, and the Department of Homeland Security. Other stakeholders were also contacted with minimal contribution.

2. Organization

The SEA-11/TDSI team members were organized into the four different threat categories (terrestrial, regional seaborne, source seaborne, port internal) according to their interests. Each individual group employed a group leader accountable to the team leader. Whether the student was in the Systems Engineering and Analysis, Sensors, Communications, Information Assurance (IA), Operations Research (OR), or Modeling, Virtual Environments and Simulation (MOVES) curriculum, integrating the students into threat categories rather than their subspecialty curricula enabled all members of the team to have an exposure to the Systems Engineering Design Process from problem definition to design and analysis. The organization structure along with the curricular make-up of each group is shown in Figure7.

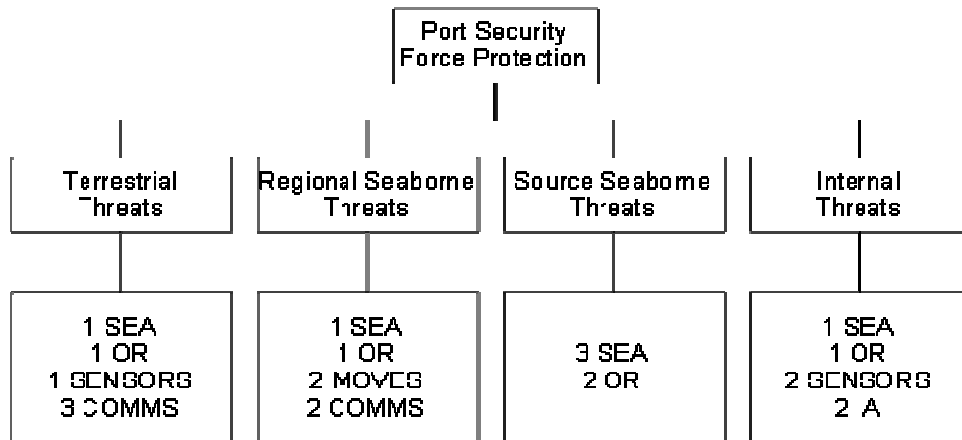


Figure 7. Port Security 2012 Organizational Layout

The Port Security 2012 organization was defined by four threat categories (terrestrial, regional seaborne, source seaborne, port internal). While each team consisted of at least one SEA member, there was an unbiased assignment of TDSI members based on curricula.

While the unbiased assignment of team members permitted the entire team to learn the fundamentals of the SEDP, this organizational structure created expertise deficiencies in some of the groups. While the IPTG had most of the information assurance students, the regional seaborne threats group did not have any MOVES personnel. Individual groups were permitted, when necessary, to seek advice and expertise from other groups and outsource their own expertise to different groups. This created an interactive culture that prevented groups from becoming isolated. Each group maintained a fundamental understanding of the purposes for each of the other groups. Meeting with the team leaders on a weekly basis, the project leader also disseminated key information to the entire team, facilitating interaction.

E. METHOD

PSS12 employed the SEDP to define, analyze, and articulate the port security and force protection issue. The SEDP consisted of three primary phases: problem definition, alternatives development, and modeling and analysis. The SEDP allowed PSS12 to look at the tasking requirements and the current situation to produce a relevant and feasible solution. When presented with the current conceptual issues, PSS12 defined the problem, analyzed the problem in terms of plausible alternative solutions, and articulated the feasible alternatives to decision-makers. It was the decision-maker's responsibility to decide which alternative, if any, should be executed. The SEDP is designed to be a cyclical and iterative process. Following execution, the SEDP could be employed again to look at the future situation to devise a better relevant and feasible solution.

Problem definition was the first and most important phase in the systems engineering design process. This phase provided the foundation in identifying the exact problem to solve. By performing the needs analysis, the group developed a clearer understanding of system components and functions necessary to carry out the desires of the various stakeholders. A clear understanding of system inputs and outputs in addition to the system composition aided in the formulation of an objectives hierarchy from which metrics were defined.

The second phase of the SEDP included the alternatives generation and the modeling & analysis processes. Several tools were used to generate all probable alternatives, eliminate infeasible alternatives, and obtain design alternatives that were able to be modeled. Using stochastic modeling through various agent-based modeling programs, measures of effectiveness for each alternative were obtained. These raw data elements were then used in the decision-making process to determine the best alternative.

The decision-making process was the third phase of the SEDP. Using alternative scoring methodologies such as multi-attribute utility theory, sensitivity analysis, and cost-benefit analysis, the measures of effectiveness amongst the different alternatives were compared and the alternatives themselves were ranked. The final decision was ultimately based on the decision-makers needs.

The final phase of the SEDP was implementation. During this phase, the decision-maker planned for action, executed the action, and constantly monitored and assessed that action. The implementation process also exceeded the scope of this project. As a new system is implemented, it could again be subject to the SEDP. The cyclic SEDP process organized and structured a problem and aided the development of a solution.

F. CHRONOLOGY

The SI3002 Project Management course from September to December 2006 established the foundation for the integrated project. The course introduced SEA-11 to the two proposed integrated projects, the requirements for each of the projects, as well as a detailed tasking letter dated December 2006. A video teleconference was held between the SEA-11 and TDSI students in November 2006 to introduce TDSI students to the two projects and their scopes. From November 2006 to February 2007, PSS12 was involved in the problem definition phase of the SEDP. During this phase, the first Interim Progress Review (IPR) was held on February 15, 2007 to generate interest and feedback, to gain subject matter expertise from faculty, and to generate collaborative work with students from other NPS departments.

Between the first IPR of February 15 and the second IPR of April 19, PSS12 executed the design and analysis phase of the SEDP. This period was focused on

alternatives generation and feasibility screening as well as learning about the modeling resources available for use. Following the second IPR, inputs were used to fully develop mature models which simulated alternative courses of action. From April 19 to mid-May, PSS12 documented performance modeling, cost benefit analysis, and scenario results. The final results were shown to the NPS community and visitors during the final presentation on May 31 and documented in the final report submitted on June 1.

In this report, four areas of port security were studied (terrestrial, regional seaborne, source seaborne, and port internal threats). The Sage and Armstrong's Systems Engineering Design Process was applied to each individual area. The three phases of the Systems Engineering Design Process are the definition, development, and modeling and analysis phases. Application of the process resulted in defining the problem for each area. The purpose of the definition phase is to identify, quantify, and clarify the need that creates the problem and determine appropriate metrics to evaluate a systems utility. It involved the identification of these needs and constraints so that a designed system may adequately address the needs whole remaining within the bounds of the constraints. The development phase involved the construction of various alternative architectures and evaluating these architectures in regards to feasibility and quality (ensuring the architectures addresses stakeholder requirements). The final stage was the modeling and analysis phase. In this phase, software models were constructed to model the architectures selected by analyzing the feasibility and quality. Some of the metrics selected in the definition phase were used to evaluate each modeled alternative. The status quo and alternate architectures were implemented in the model by varying modeling parameters. Data was collected from the model for analysis.

Following the analysis of the collected data, a cost benefit analysis of each alternative was conducted. The purpose of the cost benefit analysis was to evaluate the fiscal efficiency of each modeled alternative. From this analysis, a stakeholder may draw a conclusion of where his money would be most effectively spent.

In the final portion of this report, each group addressing the areas of port security states key findings and recommendations learned from this study.

THIS PAGE INTENTIONALLY LEFT BLANK

II. TERRESTRIAL THREATS GROUP

A. PROBLEM DEFINITION

1. Needs Analysis

a. System Decomposition

System decomposition allowed the TTG to identify the basic structure and major components of Port Security Strategy 2012. It enabled PSS12 to examine the complex interrelationships and limitations involved in handling and understanding the issues in planning, design, and management of port security. The security of a port itself was a part of enlarging security of the surrounding area. The enlarged system relative to the PSS12 included the nation's security, its economy, international trade and International Maritime Organization (IMO) standards, practices, and policies.

Critical physical infrastructure includes power stations, command centers, the main access road to the port, fuel storage/distribution location, or passenger cruise ship terminal. Power disruption on the incoming electrical supply can cripple the daily operation of the port. Any physical damage to the command center may hinder port operations and any blockage on the main axial would prevent the access to the port. An attack on a fuel storage location would likely causes severe pollution. Other physical infrastructures which are less critical include cargo cranes, cargo containers and trailer vehicles

Figure 8 displays the TTG subsystems. The Terrestrial Component consists of structural, operating and information flow within a set of boundaries restricted by the local and international policy and within the vicinity of the physical port.

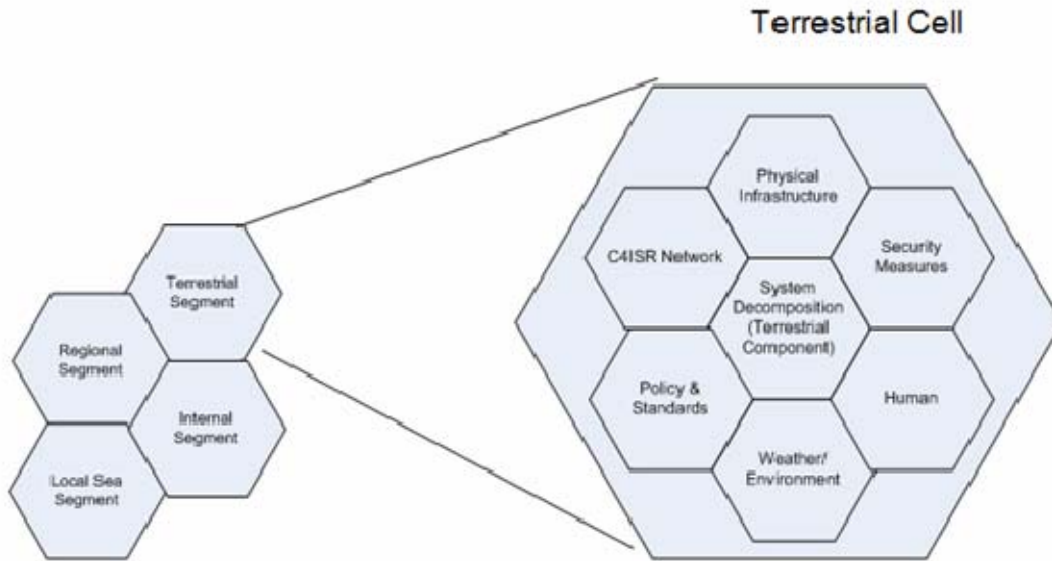


Figure 8. TTG System Decomposition

The six subsystems of the TTG are the physical infrastructure, security measures, human factors, weather & environment, policy & standards, and the C4ISR network. Each subsystem played a role in analyzing terrestrial threat scenarios.

The security measures subsystem includes private security forces hired by the port operator, Longshoremen, local police force, military force, civil defense force and security measures taken by the forces in the event of incident. The security measures subsystem includes equipment used by the security forces for port protection. Existing port security measures includes guard patrols, guard post, physical barriers, personal identification cards and closed circuit television (CCTV) surveillance. Presently, there is no impetus for port operators within the same vicinity to enhance current security measures and co-sharing of information and incident reports. The layered defense implemented by the port operators is almost nonexistent.

The human subsystem includes anyone who has dealt with the port including the Longshoremen's Union. A human subsystem is included as part of the system because human error accounts for most of the incidents and events. The cognitive thinking and behavior of humans could be influenced by psychological operation. The emotions, motives, objective reasoning, and behavior of a terrorist must be synthesized

when security measures are initiated. Including the human factor in the system enables PSS12 to address the security strategy for the port in consideration of all aspects.

The weather and environment subsystem could influence the implementation of port security measures. The performance of sensors and communication devices varies dependent upon the weather. The terrain and built up area surrounding the port can affect the link budget of the sensor as multi-path is a possibility. Weather was considered as an uncontrollable input as these conditions may influence daily operations.

The policy and standards subsystem can be classified under the local and international segments. Local policy includes port operator's internal rules, procedures, transactions and business processes. Local policies include state regulations, laws, and orders. International policies include international trade agreements, IMO standards, regional trade and co-operational agreements. The port operators must adhere to these standards and regulations in order to operate a port. International Policy and Standard was considered as a super system relative to the TTG. It was included in the studies because the terrestrial component's daily operations are affected by the international rules and standards.

The C4ISR subsystem is considered as one of the important subsystems for the TTG as the daily operations of the port depends on it. Presently, the port operator operates CCTV, High Frequency (HF) radio and walk talkie with some computers and networking devices in a stove-piped manner.

b. Stakeholder Analysis

The primary stakeholders concerned with the terrestrial threats aspect of port security are depicted in Table 4.

Authorities & Agencies	Port Operators & Users
<ul style="list-style-type: none"> • Customs/ICE/CBP • USCG • Port Authority / MPA & PSA (Singapore) • Enforcement and security agencies (Singapore) • Local Authorities • FBI 	<ul style="list-style-type: none"> • Port/Terminal Operators • Ship Owners • Private Companies • Navy Captains • Security Firms • Longshoremen

Table 4. TTG Stakeholders

The TTG stakeholders were divided into two separate categories. The authorities and agencies had specified needs and constraints, while the port operators and users had another set of needs and constraints. Most authorities and agencies are associated with a level of government. Most port operators and users are associated with the private industry.

The needs and constraints of each stakeholder can be further divided. Authorities and agencies are interested in continued port operations. From the perspective of the authorities, port operations must be maintained for region-wide economical reasons. For example, when the west coast ports of the U.S. were shut down for 10 days in 2002, it resulted in \$1B loss per day to the U.S. economy [3]. A stable and secure business environment would attract investors and promote economic growth. Hence, the safety and security of the ports, harbors, facilities, and port premises are the major concerns against terrestrial threats [15].

Security measures such as cargo checks and screenings are critical for deterring and denying terrorist threats and are of concern to port authorities and government agencies. It is desired that checks in addition to those provided by radiation portal monitors (radiation emission scanners) or similar systems be incorporated. The majority of the additional screening should be based on intelligence of possible threats. However, such measures have significant effects on the efficiency of cargo processing and shipment. The screening of each container for suspicious material would take time,

posing significant problems when all the containers are subjected to such checks. Hence, a balance of commerce and security must be achieved.

Proper access control is a vital requirement in stopping terrestrial threats. Occurrences such as Matthew Gaines' three successful attempts in port security breaches in less than six months must be avoided [16]. The access to facilities by personnel and their vehicles such as visitors, vendors, truckers, employees and longshoremen must be controlled. The implementation of biometric ID cards could minimize security breaches.

Additionally, in the event of an attack/incident, the recovery process ought to be prompt so that normal port operations could resume expeditiously. If port operations cease due to an incident and requires more than three days to recommence, it would have a national economic impact [3]. Reconstruction efforts would require consideration of economic, physical, social and psychological aspects as the port returns to normalcy. This issue has not been addressed by PSS12 because it was beyond the scope of the assigned problem.

The port operators must adhere to the security measures and guidelines laid down by the authorities in order for the overall security plan to be effective. Breaches or non-compliance to security legislation by port operators would cause a breakdown to the global security arrangement.

The protracted time required for comprehensive screening of suspicious compounds has limited the number of scans conducted. Screening systems with faster response and greater coverage could increase the screening rate.

The port operators are primarily concerned with continued operation with minimal cost while maintaining an efficient and continuous flow of cargo. Additional costs incurred in enhancing security will erode profit margin. Since the port operators are profit-conscious, it is desired that the terminals continue to operate with minimal cost. While superior security measures are welcomed, they must not result in significant delays to cargo clearance as delays will reduce profits. Hence, an efficient cargo flow is a priority among port operators.

c. Input-Output Model

The input-output model illustrates the inputs required for a system to function and the outputs a system produces. The system described here is the terrestrial security portion for the entire port. Figure 9 shows the input-output model for the TTG.

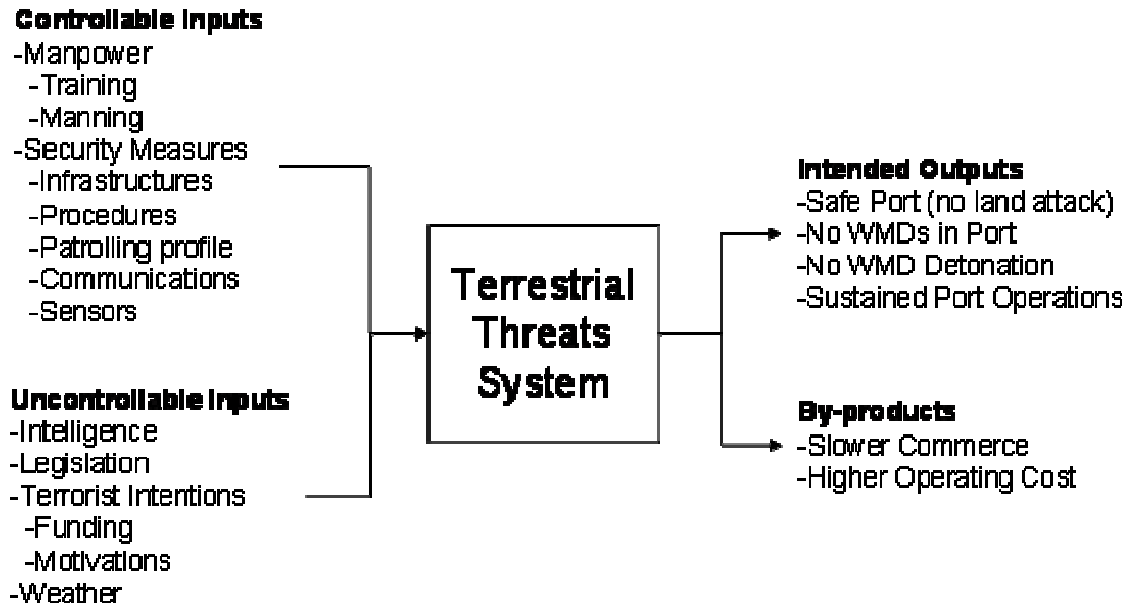


Figure 9. TTG Input-Output Model

Controllable inputs are items that are controllable by the port authority and port operators. There are two controllable inputs identified for the TTG: manpower and security measures.

The effectiveness of the security personnel and port workers is partly determined by the training received. If sufficient training on security was provided, the probability that intrusions were detected increased. The manning of security personnel is also crucial. Training and manning levels are important controllable inputs to the port's security.

The security measures undertaken by the port authority and port operators play a key role in deterring intrusions. First, the infrastructure that port operators install, such as container scanners, would help to defray intruders from planting contraband in containers. In addition, the procedures that the port authority and port operators devise,

such as the harmful items for which to scan, will determine the effectiveness of these measures. The patrolling profile of all the security personnel will aid to deter intrusions. For example, areas identified as having higher probabilities of intrusions need to be patrolled more often. Communication among the stakeholders will address the speed and effectiveness of information flow, which is critical for situational awareness. Therefore, a good and robust communications network will ensure that all stakeholders are informed of any situations in the shortest time. Lastly, the types of sensors the port authority and port operators install will help detect the occurrences of intrusions. For example, chemical sensors can help sense the presence of certain chemical compounds and initiate an alarm to alert the operators.

Uncontrollable inputs were items that are not in the domain of the port authority and port operators. There are four uncontrollable inputs identified for the terrestrial component: intelligence, legislation, terrorist intentions, and weather.

The intelligence provided by the relevant government agencies involved in intelligence gathering will be important to the port authority and port operators as it will help alert them of any potential intrusions. Port authority and port operators can thereby heighten their security measures in hoping to avert these intrusions.

The legislations that the federal and state governments enforces and determines the security measures that port authority and port operators take in order to meet the requirements.

The intentions of the terrorists and the harm they are trying to cause are correlated to the funding received and their motivation. The scale of the attack is directly correlated to the amount of funding received. For example, if terrorists have the funding and opportunity to acquire WMDs, their attack will likely be of a much larger scale than using conventional bombs.

Weather also determines the effectiveness of the in-place security measures. For example, a rain storm would greatly affect the performance of sensors or communications equipment along with the patrolling profile of the security personnel.

Intended outputs were the desired outcomes of the system which involved deterring any intrusions and keeping the port safe for prolonged operations. The identified intended outputs were a safe port with no WMDs and sustained port operations.

A safe port will increase the customers' confidence and ensures the customers continue to employ the port as a means for shipping goods. On the other hand, an unsafe port will increase insurance premiums and raise the cost of business. Customers would employ another port instead. For example, a series of intrusions causing explosions that destroyed goods would create doubt on the safety of any port. Hence, a safe port is a vital component to ensure the port's continued economic survival.

WMDs in port present enormous problems. Hence, it is crucial that security personnel maintain their vigilance in scanning for any incoming WMDs. A WMD detonation in port would cause panic and massive destruction that will take extensive amounts of time for the port to recover its operations. The customers' confidence would decline and the morale of the port workers would be negatively affected.

The port has to remain operating for the movement of cargo and the support of economic activity. A closed port would increase the transportation cost of goods coming into the region as goods would have to be transshipped elsewhere before using another mode of transport into the region. Hence, sustained port operations are imperative for commerce.

The by-products are the undesired outcomes due to the security measures implemented to enhance the security of the port. They are identified as slower commerce and higher operating cost. The installed security measures will inevitably reduce the movement rate of goods in and out of the port. Containers need to be scanned more thoroughly. Any legitimate goods that can be used for masquerading as WMDs need to be checked more frequently to err on the side of safety. All these measures will lengthen the time the container will remain in the port and therefore, slow down commerce. To enhance the security, more equipment has to be purchased and more security personnel have to be hired. Extensive training has to be provided to the port workers and more

frequent patrols have to be allotted. All of these will definitely increase the operating cost for the port authority and port operators.

d. Functional Analysis

PSS12 used functional flow diagrams to help better understand the process of functions in denial and deterrence of terrorist threats. Figure 10 shows the flow of functions for denial.

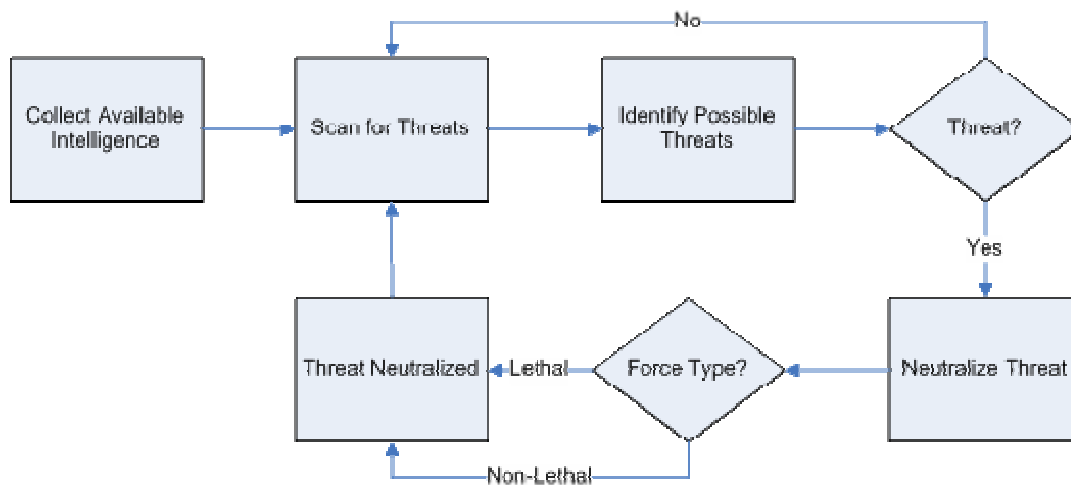


Figure 10. TTG Denial Functional Flow Diagram

For denial to be achieved, first it is essential to collect all available intelligence, then scan for threats. When a threat presents itself, it is necessary to identify the threat. If the potential threat turned out to not be a threat, the process reverted to scanning for threats. If the threat was actual, the next step was to neutralize the threat. In order to neutralize the threat, it is possible to use either lethal or non-lethal force. Figure 11 shows the flow of functions for deterrence.

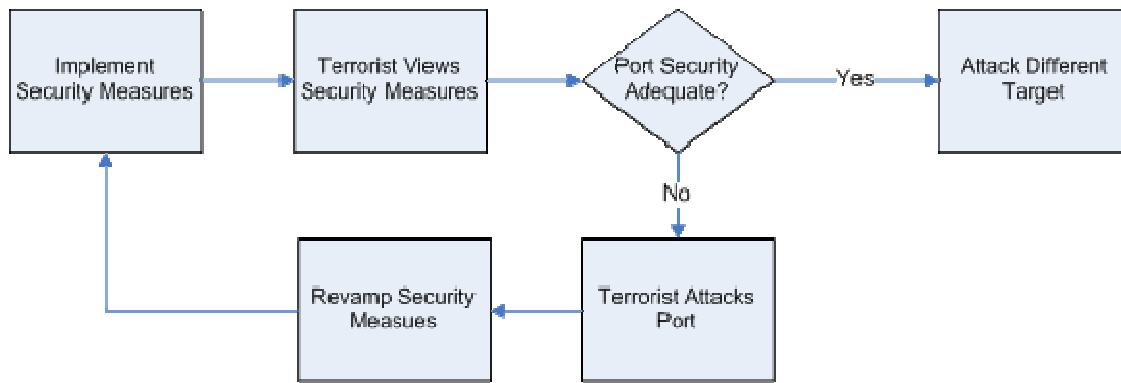


Figure 11. TTG Deterrence Functional Flow Diagram

The functional flow diagram is similar to a two player sequential game. First the port makes a decision on how much security to implement. Secondly the terrorist views the port's apparent security, and if the security was adequate the terrorist determines that attacking the port is too risky and attacks a different target. If the security is not adequate, the terrorist attacks the port. Following a terror attack on the port, the port is forced (through political pressure) to implement additional security. At this point, the process repeats with a new terrorist viewing the port's security measures.

2. Objectives Hierarchy

PSS12 uses the threats, scenarios, operational environment, system decomposition, input/output model, and the stakeholder analysis to develop an objectives hierarchy for safe port operations. Figure 12 shows the upper-level objectives for safe port operations.

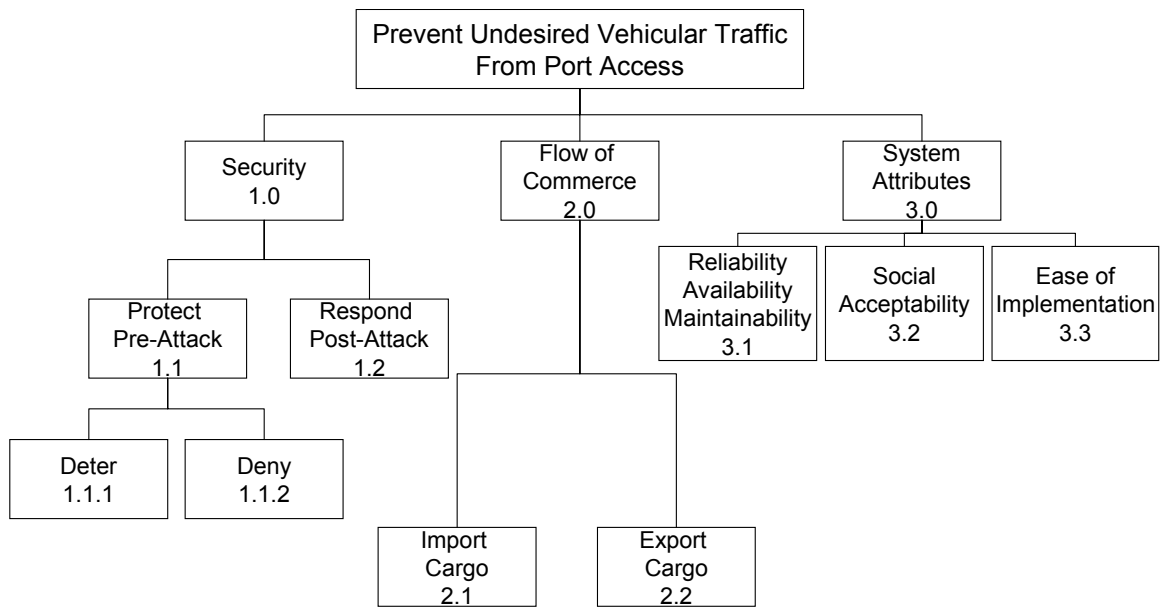


Figure 12. TTG Overall Objectives Hierarchy

The objectives hierarchy is further expanded in Figure 13 and Figure 14 with the objectives hierarchy for deter and deny. It is important to note that respond (post attack) was not further expanded because it was beyond the scope of the problem.

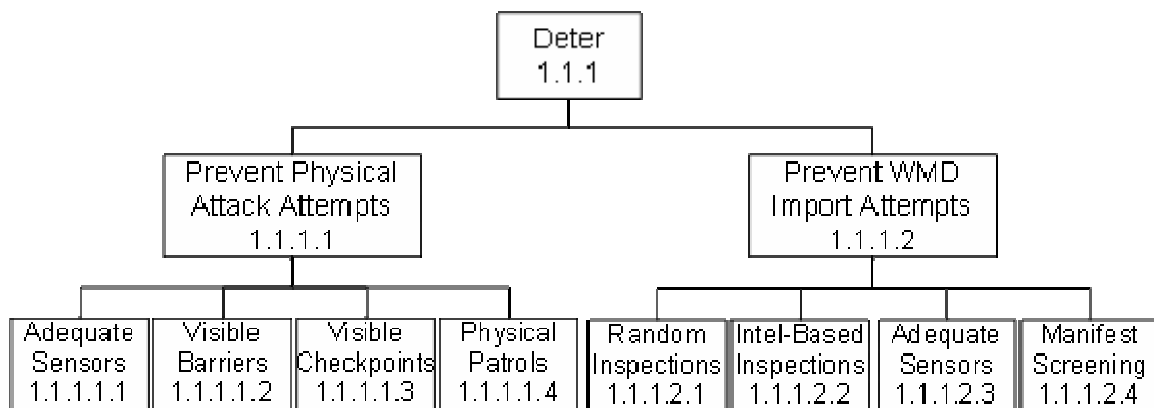


Figure 13. TTG Deter Objectives Hierarchy

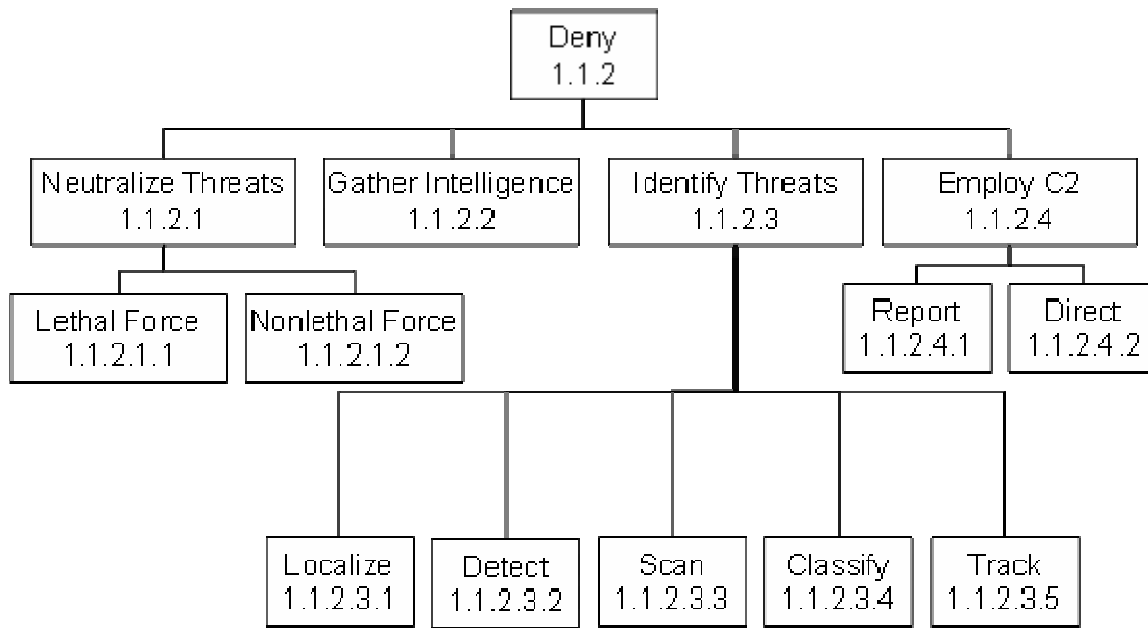


Figure 14. TTG Deny Objectives Hierarchy

The objectives hierarchy is useful because as the reader looked up in the diagram, it answers the question “why” and when looking down it answers “how.” The top objective of the objective hierarchy is to prevent undesired vehicular traffic from achieving access to the port. After PSS12 conducted its stakeholder analysis and system decomposition, it was determined that the stakeholder does not only want a safe port, but also an efficient port. This need is expressed in the next lower level of objectives which includes both port security and the flow of commerce. The flow of commerce divides into two lower end functions, import cargo and export cargo. Port security had more complex sub-objectives.

The systems attributes objectives accounted for the attributes that the stakeholders wanted in the system. The sub-objectives of reliability, availability, and maintainability, social acceptability and ease of implementation represent the properties desired in the system. The stakeholders preferred that the system perform when needed without excessive maintenance or downtime. The stakeholders wanted the system to be acceptable to the public to avoid public outcry, boycotts, or lawsuits. The stakeholders also desired the system to be easily implemented so that it would not hinder normal port operations.

The sub-objectives of security are to protect (pre-attack) and respond (post attack). Protect is described by its sub-objectives of deter and deny. Deterrence is keeping the terrorist from attempting an attack on the port, and denial is stopping an attack while in progress.

The objective of deterrence has its own objective hierarchy and its two sub-objectives which are to prevent physical attack attempts and to prevent the attempted importation of WMDs and terrorist cells. In order to prevent an attempted physical attack, it is necessary for the port to maintain the perception that it has adequate security measures. In order to accomplish this task, the sub-objective of preventing physical attack attempts is adequate sensors in place: adequate visible physical barriers, visible security checkpoints, and physical patrols. The sub-objectives of preventing attempted importation of WMD or terror cells are similar to those of prevent physical attack attempts. They include: random inspections, intelligence-based inspections, sensors (both the right type of sensors and an appropriate number), and an effective manifest screening process.

The sub-objectives of denial include: the neutralization of threats, gathering available intelligence, identification of threats, and employment of C2. In order to neutralize threats PSS12 either uses lethal or non-lethal force. The sub-objectives for identifying threats were to localize, detect, scan, classify, and track. There were two sub functions of C2 and they included report and direct.

The primary metric to be modeled is the total system effectiveness, which is defined by the number of attempted attacks that failed divided by the total number of attacks. Tracing up the objectives hierarchy, this metric measures the system performance in denying terrorists from accessing the port.

Table 5 depicts the measures of effectiveness and measures of performance that TTG can use to evaluate functional performance.

Metrics	Objective Item
Cost to Repair Damage from Attacks	Prevent Undesired Vehicular Traffic from Port Access
Number of Whole Port Equivalent Operating Days the Port is Out of Service	
Number of Successful Attacks	
Average Repair Costs per Attack	Protect - 1.1
Average Number of Whole Port Equivalent Days the Port is Out of Service Per Attack	
Number of Attacks Attempted	
Number of Attempts to Import WMDs	Deter - 1.1.1
Number of Attempts to Import Terror Cells	
Number of Successful Attacks/Number of Attempted Attacks	
Average Repair Costs per Attack	Deny - 1.1.2
Average Number of Whole Port Equivalent Days the Port is Out of Service Per Attack	
Average Number of Containers Moved Through Port	
Average Number of Containers Imported	Flow of Commerce - 2.0
Average Number of Containers Exported	Import Cargo - 2.1
Number of Unguarded Spaces Large Enough to Drive a Truck Through per Kilometer Perimeter	Export Cargo - 2.2
Number of Layers of Fence	Visible Barriers - 1.1.1.1.2
Number of Guards per Access Point	Visible Checkpoints - 1.1.1.1.3
Pop-Up Barriers (Binary)	
Number of Kilometers Patrolled per day per Kilometer Perimeter	
Percent of Containers Randomly Inspected	Physical Patrols - 1.1.1.1.4
Percent of Containers Inspected Based on Intel	Random Inspections - 1.1.1.2.1
Percent of Threats Redflagged via Manifest Screen	Intel Based Inspection - 1.1.1.2.2
Number of Threats Neutralized/Number of Attempts to Neutralize Threat	Manifest Screening - 1.1.1.2.4
Number of Threats Neutralized/Number of Attempts to Neutralize Threat	Neutralize Threats - 1.1.2.1
Number of Threats Neutralized/Number of Attempts to Neutralize Threat	Lethal Force - 1.1.2.1.1
Number of Threats Neutralized/Number of Attempts to Neutralize Threat	Non-Lethal Force - 1.1.2.1.2
Percent of Available Intelligence Gathered	Gather Intelligence - 1.1.2.2
Number of Threats Identified/Total Number of Threats	Identify Threats - 1.1.2.3
Percentage of Threats Localized	Localize - 1.1.2.3.1
Percentage of Threats Detected	Detect - 1.1.2.3.2
Total Scan Rate (km/min) per km Perimeter	Scan - 1.1.2.3.3
Total Area Scan Rate (km ² /min) per Area of Port (km ²)	
Percent of Threats Classified	
Percent Identified Threats Successfully Tracked	Classify - 1.1.2.3.4
Percent of Time Remote Communication Operational	Track - 1.1.2.3.5
Percent of Time Remote Communication Operational	Employ C2 - 1.1.2.4
Percent of Time Remote Communication Operational	Report - 1.1.2.4.1
Percent of Time Remote Communication Operational	Direct - 1.1.2.4.2

Table 5. Evaluation Metrics for TTG Objectives

It is important to note that the port equivalent operating days were a factor that accounted for the fraction of the port that was not operational for a specific period of time. For example, if 30% of the port was non operational for 10 days, the port would have been non operational for 3 whole days.

B. DESIGN AND ANALYSIS

1. Alternatives Generation

The TTG began its alternative generation phase by examining the functions that the system needs to perform. These functions are derived from the threat scenarios in the introduction. Once these functions were identified, the group used a morphological chart and divergent thinking to identify the possible alternatives for each function. Tables 6, 7, and 8 on the following page show the morphological chart developed by the TTG to address the terrestrial threat aspect of port security.

During the modeling and analysis phase of the project, the TTG scoped the problem to the “truck runs the gate” scenario. During this analysis, the TTG considered four alternatives (status quo, armed guard, spike strips, and pop-up barriers) under several different configurations described in detail in the modeling plan. The remainder of the alternative generation phase was not included in the TTG’s modeling and analysis and remained in this report to aid future study.

Truck Runs Fence	Truck Runs Gate	Truck Bomb Power Sub-station (within port)
Status Quo	Status Quo	Status Quo
Brick fence	Pop up barriers	Armed Guards
Concrete Blocks	Spike strips	Brick fence
Spike Strips	Concrete Blocks (to slow down)	Concrete Blocks
Ditch/Moat	Drop down arm	Spike Strips
Road dividers (H/W rails)	Draw Bridge	Ditch/Moat
Embankment	Armed guards	Road dividers (H/W rails)
Remote auto machine gun	EMP gun	Remote auto machine gun
	Speed bumps	Pop up barriers
Sensor - Fence	Sensor - Gate	Sensor
Status Quo	Status Quo	Status Quo
Visual	Visual	Visual
CCTV	CCTV	CCTV
Motion sensor (laser, fiber optic)	Speed detector (alarm above certain speed)	Speed detector (alarm above certain speed)
Acoustic Sensor		Negative RFID coupled with Vehicle Approach Detector
Guards tower		Sensors (for fence)
Magnetic induction detector		
Pressure sensor		
Broken wire current detector		

Table 6. Terrestrial Threats Morphological Chart (Section 1)

Truck Bomb sneaked through gate	Terrorist Importation	Nuke/Dirty Bomb Importation
Status Quo	Status Quo	Status Quo
Biometric driver ID	Increase existing random checks	Increase random checks
consolidated access list	Container embedded sensors	increase Intel based checks
at gate container inspections	Ammonia/CO2 sensors	Container embedded sensors
hand held sensors for guards	Thermal sensors	PsyOps deterrence on the level of scan check
scannable appointment ticket (for truck driver)	Air vent sensor	
Multiple layer checks	RFID on containers	
Enhancing robustness of security procedures	Weight discrepancy measurement	
RFID on trucks with cleared access	Sniffer dogs	
Sniffer dogs		
Sensor	Sensor	Sensor
Status Quo	Status Quo	Status Quo
Biometric driver ID detector	container sensors	
Explosives detection system (dogs, handheld sensor etc)	ammonia sensors	
Receiver for transponder on trucks	thermal sensors	
RFID transceiver	magnetic anomaly sensors (to detect electronics)	
	air vent sensor	
	RFID transceiver	

Table 7. Terrestrial Threats Morphological Chart (Section 2)

Chemical/Biological importation
Status Quo
Increase random checks
increase Intel based checks
Increase # available sensors
Container embedded sensors
PsyOps deterrence on the level of scan check
Sensor
Status Quo
Chemical swab detector

Table 8. Terrestrial Threats Morphological Chart (Section 3)

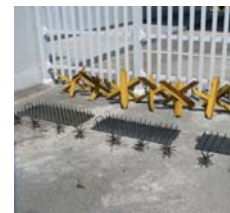
In most cases, after the alternatives addressing each function of the system were generated in the morphological chart, each function was linked to form a complete alternative. The TTG did not link the different function alternatives together to form complete alternatives because each function alternative was assumed to be a stand alone subsystem that had little dependence on the other elements of the system. When combining all possible permutations of alternatives, there were tens of thousands of alternatives. This vast number made selecting complete alternatives unrealistic. Instead of examining complete alternative systems, the TTG decided to look at each function alternative individually. This method would allow the group to select the best alternative for each function and then link the optimal subsystems together to form the optimal complete system. It is important that to note that each proposed alternative was in addition to the status quo, and in under no circumstances would the security be reduced from the status quo.

a. Truck Running Fence Scenario

In this scenario, the perpetrators attempt to make a forced entry into the port by penetrating the perimeter fence. If the perimeter protection of the port is weak and the attackers have no reason to make a stealthy entry into the port, this scenario is plausible. An example is a suicide bomber in a vehicle bomb employing this method of entry to get to his target within the port. Commercial perimeter fence is composed of a single layer of chain-link (mesh) fence that could not withstand a large impact force. If a heavy vehicle, such as a full-size truck, impacted the fence with sufficient momentum, it could easily penetrate the fence.

To prevent this scenario from happening, the perimeter fences of the ports need to be strong. There were several alternatives than enhanced the strength of the perimeter barriers. They could have been implemented as a replacement to existing defenses or added to existing defenses to make them stronger. Combinations of them could have also been implemented to form a layered defense.

- *Concrete Fence.* Concrete walls can be erected along the entire perimeter of the port, instead of the chain-link fence. They are structurally stronger than chain-link fences, however they are more expensive.
- *Concrete Blocks.* Concrete blocks can be used in combination with chain-link fences. They would be lined outside the fence to form an additional layer of barrier that is heavier and sturdier.
- *Road Rails.* Road rails, similar to those used along highways, can be used to complement existing chain-link fences. They can be constructed alongside the existing fences.
- *Spike Strips.* Spike strips can be used to line the perimeter to stop vehicles by puncturing the tires. They can be used to complement the existing chain-link fence.
- *Ditch/Moat.* A ditch or moat bordering the perimeter of the port can be used as a barrier. It would have to be physically wide and deep enough to stop a vehicle trying to breach it. This method would occupy much space when installed.
- *Embankment.* An embankment is a barrier made of earth wall. Just like the ditch/moat, it would occupy much space when installed and also it would have had to be high enough to stop a truck.
- *Remote Machine Gun.* A weapon system can be strategically positioned along the perimeter to neutralize any vehicle that attempted forced entry.



b. Truck Running Gate Scenario

Similar to the scenario of truck penetrating fences, threats could have also made a forced entry into the port by driving through the gates. Gates with simple barriers like “drop-down” arms were generally inadequate against any deliberate forced entry. To reduce the possibility of such a scenario requires measures that accomplish two things. First, the measures have to be able to effectively slow down any vehicles approaching the gates. Secondly, the measure has to be able to effectively stop or prevent any vehicle that attempted to crash through the gates.

The alternatives are shown below. Several of them are similar to those presented for the Truck Runs Fence scenario. They can be implemented individually or combined to form a more effective layer defense.

- *Concrete Blocks.* Concrete blocks can be arranged in a formation at the final approaches to the gates. They serve to force vehicles to slow down while approaching the gates.
- *Spike Strips.* Spike strips can be used to stop vehicles by puncturing the tires. They can be activated manually or automatically when a vehicle attempts to run through the gate.
- *Pop-up Barriers.* Pop-up barriers could be embedded in the road, usually immediately after the gate. They can be activated remotely when a vehicle makes a forced entry. These barriers would stop vehicles from advancing further by puncturing tires, presenting a strong barrier such as bollards, etc.
- *Drop-down Arm.* Though drop-down arms are generally ineffective against forced entry, they serve the purpose of clearly indicating a controlled access through the gate. They provide a convenient way of controlling flow through the gate and make any attempt of forced entry more obvious.



- *Draw Bridge.* A draw bridge would be very effective in preventing entry through the gate if it can be drawn before the attackers reach the bridge.



- *Armed Guards.* The existing guards at the gates can be equipped with firearms. The firearms could be fired at the intruding vehicles to immobilize them.
- *Speed Bumps.* Speed bumps are used to force vehicles to reduce their speed while approaching the gate. By slowing the speed of approach, the vehicle had less momentum to crash through the gates.



- *Electromagnetic Pulse Gun.* EM pulse can be used to cause the electronic circuitries onboard vehicles to malfunction, causing the vehicles' engines to shut down. This technology is not yet mature.

c. Truck Bombing Power Substation Scenario

This scenario was similar to the two above, but it was made under the assumption that a truck with a bomb had penetrated the port's perimeter and intended to attack the port's critical infrastructure which could include a power substation, fuel storage/distribution location, or passenger cruise ship terminal. All of the alternatives for this scenario were similar to those for the previous two scenarios, but instead of protecting the entire port perimeter, they kept the truck from reaching the critical infrastructure (power substation).

d. IED Smuggled Through Gate Scenario

In this scenario, the terrorists would attempt to enter the port legitimately under the cover of disguise and/or false pretence. The attacker driving the truck could be an employee of a trucking company who had infiltrated into the trucking network for the purpose of a terrorist act in the port. The terrorists could also be disguised with forged documents. There is the possibility of assistance from within the port if the terrorists have

infiltrated into the port security network. A sizable amount of explosives would have to be smuggled into the port by the attackers.

The solutions to this scenario address two issues. First, the integrity of the security procedures at the port entrance have to be intact at all times. The procedures have to be robust to prevent attackers from infiltrating with forged documents and insider help. Next, the checks and inspections measures at the port entrance must have a high probability of detecting explosive devices.

- *Biometric Driver ID.* All authorized truck drivers would have biometric identifications. These IDs would allow for the matching of the drivers' biometric data with the security system's data. These features would make forgery difficult.
- *Consolidated Access Lists.* These lists serve to enhance the robustness of port security measures. It is a list containing information on authorized entries into the port for a given day. The lists could have information such as the driver's information, truck license number, and cargo manifest. Any driver and/or truck not listed will be subjected to more stringent checks and inspections. The list can be complemented by a barcode appointment ticketing system. This is an appointment slip with barcode for all trucks that are scheduled to enter the port. Barcode scanning allows for a faster rate of processing.
- *Multiple Layer Checks.* This serves to enhance the robustness of port security measures. Multi-layered checks remove the reliance on a single point of defense. The probability of the perpetrators slipping through a few layers of defense would be less than that of a single layer of defense.
- *Radio Frequency Identification (RFID) on Trucks with Cleared Access.* Trucks certified for access into the port would be tagged with RFID. This system allows for the quick processing of incoming trucks when scanning for unauthorized trucks that attempt to sneak into the port.

- *Container Inspections at Gates.* Inspections of containers can be conducted at the gates. The inspections can be done by x-ray machines which are less labor intensive and have a faster processing rate than humans. Inspections can be carried out by guards, but it would be more labor intensive and much slower.
- *Handheld Sensors for Guards.* Guards could use handheld explosive detectors to scan for hidden explosives in trucks.
- *Dogs.* Dogs can be used to detect certain explosives in trucks.

e. Radiological Weapons Scenario

The international Nuclear Non-Proliferation Treaty (NPT) was initiated for countries to commit themselves in limiting the spread of nuclear weapons since 1968 [17]. Not all countries have endorsed this treaty. The smuggling of nuclear bombs by terrorists into a country is less likely as considerable international efforts and policy such as NPT have been put in place to reduce the proliferation of nuclear weapons and material. Nevertheless, sufficient measures have to be implemented in case a radical state in possession of nuclear weapons decided to support a terrorists group. Failure to detect nuclear weapons importation will result in tremendous consequences.

Radiological Dispersal Devices (RDD), commonly known as dirty bombs, are different from nuclear bomb because they do not use fission or fusion to produce an explosion; however, they use conventional explosives to scatter radioactive material in order to contaminate a large area. Based on the United States Regulatory Commission (URC), more than 2100 organizations in the state are licensed to use radioactive materials [18]. Therefore, the possibility of terrorists obtaining the radioactive material combined with a detonator to form a dirty bomb does exist. Dirty bombs are considered WMD because they cause extensive economic damage, through the expensive cleanup required following an attack, and by preventing real estate from being used for its intended purpose. The detonation of a dirty bomb would also result in illness of the victims within the vicinity. The physical damage caused would not be catastrophic. It would create

inconvenient, massive disruption and adverse psychological effects on the victims as well as contaminate a large area, resulting in large economic losses.

Detecting radioactive materials has always been challenging. Nuclear weapons contain large amounts of plutonium and uranium required for nuclear fission [19]. The weapons grade plutonium and uranium are very dense and exhibit unique properties. There are three basic ways of detecting these materials based on their properties. Passive detection of the radiation emitted by these radioactive materials, active detection involving radio-graphing (“x-raying”) the materials, and irradiating an object with neutrons or high energy photons and detecting the particles emitted by the resulting induced fissions. The first method is the safest but least efficient as it may be evaded by terrorists. The second method can overcome some evasion but it is costly, inconvenience and complicated. The third method poses a human safety risk.

According to the CBP website, CBP operates the following inspection and surveillance technologies to detect nuclear and radioactive materials [20]:

- *Radiation Portal Monitor (RPM)*: A passive, non-intrusive means to screen trucks, cargo containers, vehicles, and other conveyances for radiation emanating from nuclear devices, dirty bombs, special nuclear materials, natural sources, and isotopes.
- *Personal Radiation Detector*: A small, but highly sensitive, device carried by CBP officers at ports of entry and CBP Border Patrol agents at highway checkpoints. It will sound an alarm if radiation is detected during an inspection
- *Radiation Isotope Identifiers*: A hand-held instrument capable of detecting gamma and neutron emissions from radioactive sources, including nuclear, medical and industrial isotopes. CBP officers use this device to determine the exact identity of a radioactive source causing an alarm
- *Large-scale Gamma-ray/X-ray Imaging Systems*: Produce transmission and reflected images of the contents of a cargo container, rail car, vehicle or trailer-truck. CBP officers analyze these images to determine where there are anomalies associated with the cargo listed on the manifest. There are 166 systems in use, with more to be added shortly.

The CBP works closely with the port operators, port authority, USCG and other agencies and use the most recent technology for the detection of nuclear and radioactive materials at the various check points. In addition, they have implemented a layered defense security strategy by extending the surveillance zone to the host countries through the Customs-Trade Partnership Against Terrorism (C-TPAT). These initiatives and activities have hardened the security of the border but presently not every port is equipped with the same capability. To deter and prevent the smuggling of radio active materials, every port needs to be equipped with the nuclear and radioactive detectors.

Alternatives for detecting the importation of radioactive material are as follows:

- *Status Quo*. All containers are scanned for radioactive cargo before leaving the source port. Detection of radiation triggers further screening.
- *Increase the number of in-depth inspections*. These inspections could be both intelligence based or completely random
- *Smart Container*. The general purpose containers usually come in standard sizes. The container number and owner information are displayed on the external wall of containers. A sensor integrated with radio frequency could be housed inside of a container to detect radioactive material. If the container detects radiation, it would signal that it requires additional screening.
- *Psychological Operations (PSYOPS)*. PSYOPS are planned operations to convey selected, truthful information and indicators to foreign audiences to influence the behavior of their governments, organizations, groups, and individuals favorable to the originator's objective [21]. The methods of delivering PSYOPS could be through email, leaflets, TV broadcast and radio. In this context, PSYOPS could be implemented within the port to mislead terrorists, making them believe that every port is equipped with adequate biological, chemical and nuclear sensors. This likely would deter many terrorists from using the port as a means to smuggle WMDs.

f. Biological and Chemical Weapons Scenario

Biological and chemical weapons are considered WMDs. The 1925 Geneva Protocol and 1972 Biological and Toxin Weapons Convention treaties restrict countries from acquiring, developing, stockpiling biological agents outside of peaceful purposes [22]. However, not every country signed these treaties.

Detecting biological and chemical weapons at the port proves to be a challenge since a small amount of these microorganisms and materials can be easily concealed. Nerve agents such as VX and biological agents such as anthrax are extremely lethal and pose a significant risk as terrorist weapons. The material and equipment used for biological and chemical weapons production are similarly used for normal scientific research as well. According to Dr. Kosal, the detection of chemical and biological agents proves to be almost impossible for “detect to warn” scenario when the agents or chemicals are contained in a sealed environment [23]. Evaluation time for some of the biological bacteria could exceed 24 hours. In addition, there is no single detector that can be used to detect various biological and chemical weapons because of their unique characteristics and each detector has its own drawbacks and limitations. Nevertheless, appropriate biological and chemical detectors must be used in port to detect any leakage or smuggling of such materials.

Alternatives for detecting the importation of chemical and biological weapons are as follows:

- *Status Quo.* In depth screening of random containers as well as containers that CBP determined to be of increased risk through a manifest screening process.
- Increased in depth inspections. These inspections could be both intelligence based or completely random.
- *Smart Container.* A sensor integrated with radio frequency can be housed inside a container to detect chemical and biological compound. Some nerve agent gases are denser than the others and exhibit certain properties when released. Therefore, the placement of sensor within the container needs to be studied for

effective detection. When the sensor detects some abnormality, it would send the information to the nearest base station to alert the authority.

- *PSYOPS*. The same as PSYOPS previously discussed in the radiological weapon section.
- *Increase the number of sensors available to CBP*. This alternative required CBP to procure more chemical and biological sensors and to use these sensors to screen imported cargo.

g. Terrorist Cell Importation Scenario

In this scenario, a terrorist organization attempts to import a terrorist cell inside a modified cargo container. The successful importation of terrorists would allow the cell uncontrolled access to the importing country, where they would present a substantial threat to the populace and infrastructure.

Alternatives for the terrorist cell importation scenario are as follows:

- *Status Quo*. In depth screening on random containers as well as containers that CBP determined to be of increased risk through a manifest screening process.
- *Increase the number of in-depth inspections*. These inspections could be both intelligence based or completely random
- *Smart Container*. A sensor could be housed inside a container to detect the presence of personnel.
- *Weight Discrepancy Measurement*. This alternative requires that each imported container be weighed, and its weight compared against the anticipated weight of the container based on its manifest.

h. Sensor Solution Alternatives

This section includes the available sensor alternatives to prevent or detect the occurrence of the above scenarios. It is important to note that several of these sensors are part of the status quo and others would be useful additions to those currently employed.

Truck Running Fence Sensor Alternatives

- Visual
- Guard Tower
- Intrusion Location and Video Assessment System (RBtec VIDAlert System) [24]

(1) This is a PC-based Intrusion Detection & Video Monitoring System is capable of integrating with other sensors, thus fulfilling the operational need for intrusion detection and video assessment.

(2) Any intrusion attempt is identified by a real-time presentation of alarms and video picture by automatic synchronized camera movement in the direction of the affected alarm zone. The intruder's picture is presented either in motion or in still "freeze" mode and is stored in the computer's memory, for later recall and printing.



Figure 15. VIDAlert CCTV System

- Microphonic Cable Fence Disturbance Sensor (IntelliFLEX) [25]
- (1) IntelliFLEX uses microphonic intrusion detection for outdoor, fence-mounted perimeter security applications. Utilizing signals generated by the minute flexing of a coaxial sensor cable, specific characteristic

intrusion signatures are analyzed. It could detect an intruder cutting through, climbing on or lifting the fence fabric.

(2) Each IntelliFLEX zone (two per Signal Processor) could protect approximately 950 ft of eight ft high metal fabric fence. For fences up to 12 ft, a double pass of the cable at equal vertical distances is required. In most cases, facility perimeters were configured in shorter zones to match CCTV assessment capabilities and to allow rapid response to the area of attempted intrusion.

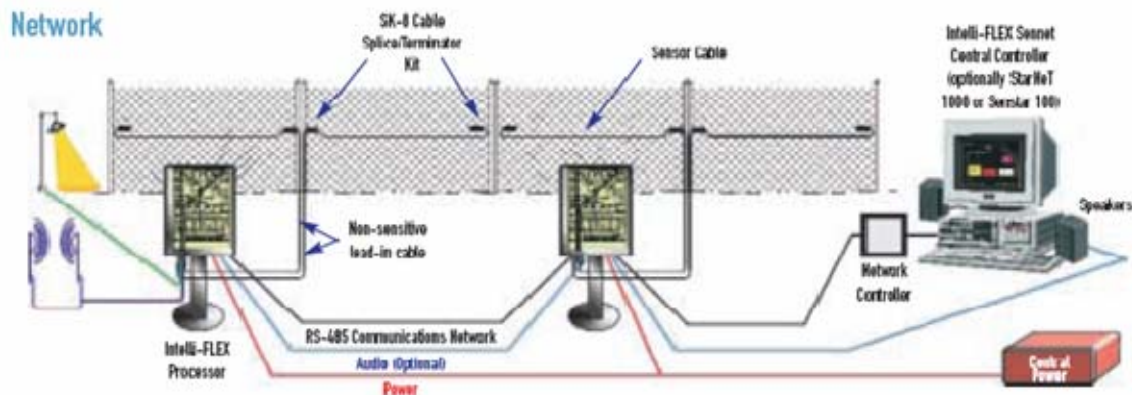


Figure 16. Intelli-FLEX Network Configuration

- Fiber Optic Cable Fence Disturbance Sensor (IntelliFIBER) [26]

(1) IntelliFIBER uses fiber optic intrusion detection for outdoor, fence-mounted perimeter security applications. Utilizing signals generated by the minute flexing of a fiber optic sensor cable, IntelliFIBER can detect an intruder cutting through, climbing on or lifting the fence fabric.

(2) Each IntelliFIBER zone consists of up to 3280 ft of fiber optic sensor cable. A single pass of cable is required to protect an eight ft high metal fabric fence. For fences up to 12 ft, a double pass of the cable at equal vertical distances are required. In most cases, facility perimeters are configured in shorter zones to match CCTV assessment capabilities and to allow rapid response to the area of attempted intrusion.

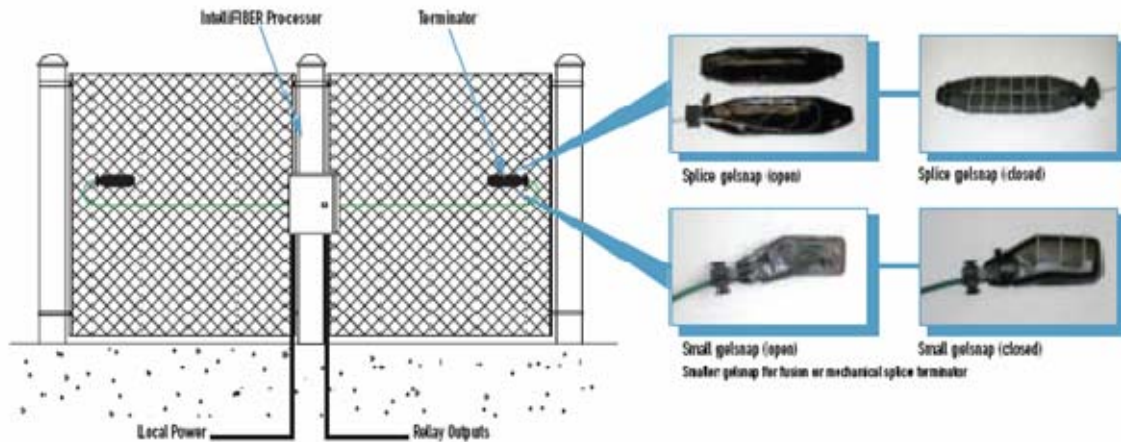


Figure 17. Intelli-FIBERT Configuration

- Buried Cable Intrusion Detection System (Perimitrax) [27]

(1) Perimitrax is a covert perimeter intrusion detection system based on an invisible electromagnetic field around buried sensor cables. If an intruder disturbs the field, an alarm is sounded. It uses a large volumetric field to detect moving targets based on their electrical conductivity, size and movement. A person or vehicle crossing through the field is detected while small animals and birds are ignored. Common environmental false alarm sources like foliage, rain, snow and blowing sand are easily filtered out by advanced adaptive algorithms.

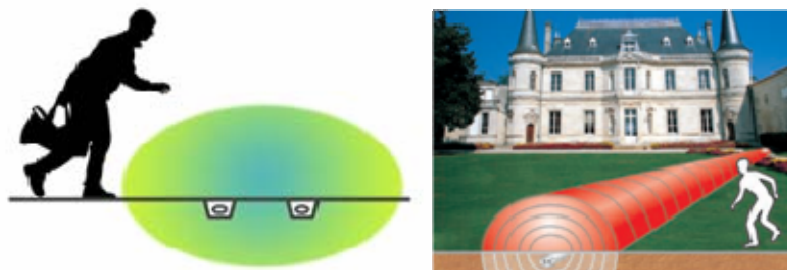


Figure 18. Perimitrax System

- Electrostatic Field Disturbance Sensor (IntelliFIELD) [28]

(1) IntelliFIELD is a terrain-following, volumetric sensor that creates an electrostatic field between parallel field and sense wires. An intruder is detected when the electrostatic field that is created between field and sense wires is disturbed. The wires do not need to be touched in order to disturb the field. The wires could be mounted on freestanding poles, walls, roofs, fences or other structures to provide a high, narrow field of detection.



Figure 19. Intelli-FIELD System

- Microwave Protection System (IntelliWAVE) [29]

(1) The IntelliWAVE microwave intrusion detection sensor is a volumetric, high-performance system that creates a microwave field between transmitter and receiver units in order to detect intruders based on their size and speed.

(2) It uses a separate transmitter and receiver and is installed inside of a physical barrier, such as a fence or wall. Since the detection field is quite large, the sensor is difficult to avoid or defeat. Because of their modest cost, microwaves are frequently used for short zones at gates in place of a higher cost sensor.



Figure 20. Intelli-WAVE System

Truck Running Gate Sensor Alternatives

- Visual (as per Truck Runs Fence Scenario)
- CCTV (as per Truck Runs Fence Scenario)
- Speed Camera (RedFlex Lasercam) [30]

(1) Redflex's Lasercam Speed Camera System combined digital image capture with highly accurate laser speed detection. Lasercam™ captures two images of an infringing vehicle concurrently; a wide angle lens captures an environmental image of the vehicle in its immediate surroundings and a telephoto lens captures a close up image of the vehicle

and its registration plate. This ensures effective identification of a targeted vehicle at all times.



Figure 21. RedFlex Lasercam System

Truck Bombing Power Substation Sensor Alternatives

- Visual (as per Truck Runs Fence Scenario)
- CCTV (as per Truck Runs Fence Scenario)
- Speed Detector (as per Truck Runs Gate Scenario)
- RFID Cargo Tag [31]

(1) The Cargo Tag is an all-weather RFID tag with the durability required for 24-hour, outdoor exposure in most environmental conditions. It delivers accurate and reliable read performance of up to 40 ft, thus achieving maximum benefits in RFID cargo and asset tracking applications.

(2) The tag is tuned to utilize its aluminum backplate to improve the signal. The integrated antenna is designed to deliver superior read range. Additionally, since there is no battery to change, this passive tag is maintenance free and there is no loss of read capability due to a dead tag battery.



Figure 22. RFID Cargo Tag

Truck Sneaking Past Gate Sensor Alternatives

- Biometric ID System for Truck Drivers [32]

(1) Fingerprint Identification. Fingerprint identification involves comparing the pattern of ridges and furrows on the fingertips, as well as the minutiae points (ridge characteristics that occur when a ridge splits into two, or ends) of a specimen print with a database of prints on file. Good fingerprint scanner technology is readily available. However, it might not work in industrial applications because it requires clean hands.



Figure 23. Fingerprint Identification (DHS IDENT System)

(2) Hand Geometry Biometrics. Hand geometry readers work in harsh environments, they do not require clean conditions, and form a very small dataset. It is not regarded as an intrusive test. This is often the authentication method of choice in industrial environments.

(3) As the human hand is not unique, the finger length, thickness, and curvature could be used for verification but not for identification. However, it is possible to devise a method by combining various individual features to attain robust verification. Hence, it can be envisioned that fingerprints are used for (infrequent) identification and hand geometry was used for (frequent) verification.

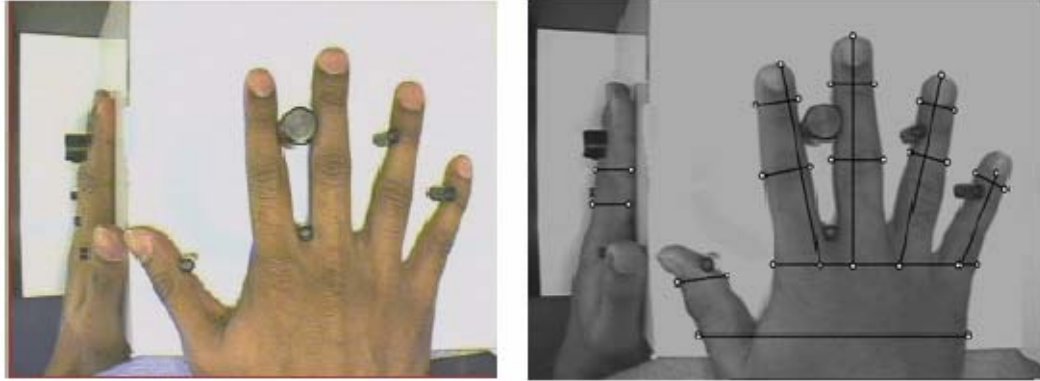


Figure 24. Hand Geometry Biometrics

- Vehicle Explosive Detection System (Rapiscan Systems Neutron Scanner) [33]

(1) The Vehicle Explosive Detection System is an automatic, non-intrusive inspection system that detects explosives and chlorinated forms of class-A explosives. The neutron inspection technology is unique in providing material specific detection, and is well suited to meet the requirements for protection against terrorist vehicle bombs.

(2) The neutrons create gamma-ray signals when they interact with the elemental ingredients of the inspected object. The gamma-ray energies are unique to the elements in the inspected object. If the gamma-ray signatures match those in a threat database, the system automatically triggers an alarm indicating the possible presence of the threat.



Figure 25. Vehicle Explosive Detection Systems

- Hand-Held Trace Detector (SABRE 4000) [34]

(1) This is capable of detecting threats from explosives, chemical warfare agents, toxic industrial chemicals and narcotics. It can detect and identify over 40 of these threat substances in approximately 15 seconds. It

is capable of analyzing either trace particle or vapor samples, allowing the operator to apply the ideal sampling technique for the suspicious substance.



Figure 26. Hand-Held Trace Detector

- RFID Reader (Symbol XR400) [35]

(1) The RFID fixed reader is designed to function as part of a complete RFID system for accurately tracking the location and status of inventory and assets. It has the ability to read, update and transfer RFID tag information in real time to the enterprise systems.

Terrorist Cell Importation Sensor Alternatives

- Heartbeat Detector (Advanced Vehicle Interrogation And Notification System) [36]

(1) This system detects the presence of people hidden in vehicles. Using data from special sensors, it finds the shock waves generated by the beating heart, which coupled to any surface or object with which the body is in contact. AVIAN collected the data and analyzes it using advanced signal processing algorithms to detect a hidden person in less than 1 minute. It is a cost effective method to accurately and quickly search vehicles, regardless of contents, for hidden persons.

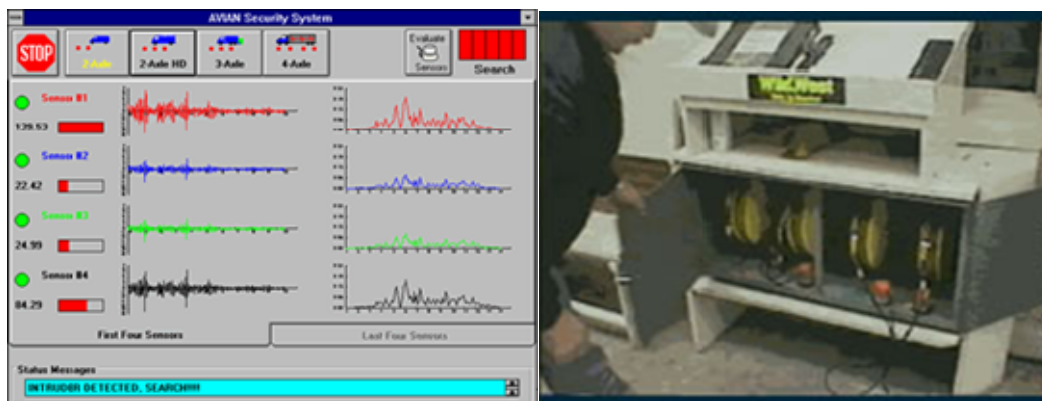


Figure 27. AVIAN Heartbeat Detector

- Carbon Dioxide Sensor [37]

(1) This is designed to measure the carbon dioxide concentration in a confined environment. In a normal outdoor environment, the level of carbon dioxide is approximately 400 ppm. In the event that people or living creatures are inside a container, they would exhale carbon dioxide and its concentration would increase to a higher level depending on the number of living beings and the duration of stay within the container. The measurements could be obtained by inserting a sampling probe into the container for three minutes without opening the door.

- X-ray Scanner (Rapiscan Systems) [38]

(1) High energy X-ray systems are designed to meet the full range of cargo inspection applications. The linear accelerator X-ray sources can penetrate dense cargo. The resulting high quality images enable inspectors to detect hidden contraband including weapons, explosives, weapons of mass destruction, drugs, and undeclared goods.

(2) Such scanners can be Mobile Systems (truck-mounted, road mobile and easily relocatable), or Gantry and Portal Systems (drive-thru portal system for trucks).



Figure 28. X-Ray Scanners

- Gamma-Ray Scanner (Rapiscan Systems) [39]

(1) Gamma-Ray systems have an intrinsically lower radiation field when compared to equivalent X-ray systems. This provides a smaller operational area and exclusion safety zone. While such systems require less maintenance and lower cost of ownership than equivalent X-ray systems, the radioactive source (Cobalt-60) requires replacement every five years. They are designed to detect hidden contraband including weapons, explosives, weapons of mass destruction, drugs, and undeclared goods.

(2) Such scanners could be Mobile Systems (provides the greatest operational versatility), Gantry Systems (provides complete inspection of stationary and unmanned vehicles, cargo and palletized materials) and Portal Systems (High inspection throughput is achieved with the drive-through).



Figure 29. Gamma Ray Scanners

- RFID Reader (as per the IED smuggled through gate scenario)

Radiological Weapons Sensor Alternatives

- Vehicle Explosive Detection System (as per the IED smuggled through gate scenario)
- Radiation Portal Monitor (SAIC AT-900 Series) [40]

(1) The Radiation Portal Monitor (RPM) is a complete vehicle monitoring system used for the rapid detection of unknown hidden radioactive sources in moving vehicles. A full color console guides a gatehouse operator to each radiation alarm, linking the alarm to a passing vehicle.



Figure 30. Radiation Portal Monitors

Biological and Chemical Weapons Sensor Alternatives

- Hand-Held Trace Detector (as per the IED smuggled through gate scenario)

According to Dr. Kosal's paper, the following sensors are available for biological and chemical weapon detection; however, the majority of these sensors are not currently feasible for detecting chemical and biological weapons in shipping containers [23].

Biological detectors include the following:

- Pointer Detection
 - Aerosol Particle Sizers (APS)
 - Immunoassays
 - Genetic Detection
 - Mass Spectrometry
 - Surface Acoustical Wave Sensors
- Remote Detection
 - Cloud Recognition via Light Detection and Ranging (LIDAR)
- Biowatch

(1) Biowatch is a biological detector network constructed by US Department of Homeland Security with Environmental Protection Agency and the Centers for Disease Control to analyze the contents of the atmosphere for biological weapon agents.

Chemical weapon detectors available for detecting different types of chemical compounds include [23]:

- Pointer Detection
 - Colorimetric Indicators
 - Electrochemical or chemiresistor detectors
 - Ion Mobility Spectrometry
 - Mass Spectroscopy with gas chromatography
 - Flame Photometry
 - Photoionization
 - Surface Acoustical Wave Sensors
 - Enzyme-Based Detector

- Non-Destructive Evaluation Sensor
 - Isotopic Neutron Spectroscopy
 - Standoff Detector
 - Infrared Spectroscopy
 - Raman Spectroscopy

C. MODELING AND ANALYSIS

1. Modeling Plan

The TTG began the modeling and analysis phase of the project by examining the threat scenarios presented earlier in the paper. After considerable thought, the TTG broke the threats into two separate groups for potential modeling. The two groups were imported container screening models and perimeter/gate security models. After further investigation, the TTG decided that modeling the perimeter security would prove more useful than attempting to develop a container screening model. The TTG came to this conclusion because there is considerable work currently being done on container screening, both in the U.S. and around the world. The TTG also concluded that it would be more useful to model perimeter security because accurately modeling domestic container screening would require the use of classified material, which is beyond the scope of this paper. It is noteworthy to mention that Sandia National Laboratories has developed a classified container screening model that potentially could be used for classified research.

Further examination of the potential modeling for perimeter security led the TTG to decide to model gate security. This decision was based on the logic that modeling improvements in security to protect critical infrastructure are overly sensitive to the particular infrastructure's vulnerability to blast weapons, and given its vulnerability, one can simply use a chart to predict the damage caused by a given amount of explosives at a set range. With this established, a large amount of explosives, perhaps in a container carried by a semi truck, would likely have a devastating effect on most targets at ranges into the hundreds, if not thousands of feet. This fact, coupled with the economic value of land on port facilities, makes it likely unrealistic to cordon off thousands of square feet of prime property, in order to protect critical infrastructure from blast weapons. The TTG

also decided that modeling the alternatives for hardening the port's fences also prove less useful than modeling gate security. It is essential that all of the ports perimeter fences first be hardened before additional security measures are added to the gates. If the gates have adequate security, but the fences are not hardened, a terrorist with a vehicle-born IED will likely drive through the unhardened fence. Once the perimeter fences are adequately hardened, the terrorist would either be deterred completely, or would be forced to attempt gain entry to the port through the ports gates.

Given that the TTG intended to model gate security, it had to decide between modeling a vehicle attempting to gain access covertly (sneak in past the guard), or modeling a vehicle attempting to drive through the gate security at the highest speed possible. The TTG decided to model the scenario in which a truck laden with explosives attempts to drive through the gate security measures as quickly as possible, in hopes of gaining entry to the port terminal before the defensive measures could be effectively employed. Once on the port terminal the explosives laden truck would then proceed to critical infrastructure, or a high value target on the terminal, and detonate itself.

After choosing a suitable scenario to model, the TTG developed its modeling plan. The key metric modeled by the TTG was the system effectiveness, which satisfied the objective of denying terrorists access to the port. Alternatives modeled included:

- status-quo (for the Port of Oakland)
- pop-up barriers
- spike-strips
- armed guards (to shoot out the tires of vehicle born IEDs)

It is note worthy to point out that the TTG decided not to model the effectiveness of drop down arms, as this type of a device would create a delay for trucks entering the port during normal operations. In addition to modeling the listed alternatives the TTG thought that it would also be useful to model the effects that staggered concrete blocks (to force incoming vehicles to reduce their speed) would have on the effectiveness of the modeled alternatives. The three alternatives for the concrete blocks were no blocks, blocks before the initial guardhouse, and blocks just before the barrier. The TTG also decided to model the impact that varying the distance of the security zone would have on the effectiveness of the alternatives. The security zone is defined as the distance between

the guard house and the defensive measure (pop-up barrier, spike strips, armed guard). The purpose of varying the distances as well as the alternatives is to provide generic results that are useable for the gate to any port terminal, regardless of physical constraints. Appendix A, Table A1 shows a list of complete alternatives, including different defensive measures, concrete block positions, and distances, which the TTG intended to model. It is note worthy that replications 31-50 were only going to be modeled if it was later desired to add more clarity to results 1-30.

2. Modeling Explanation

The TTG took its modeling plan and researched several different simulation options to determine which software/technique would work best for modeling gate security and provide the TTG with the primary MOE for system performance. The TTG determined that its best option for modeling gate security would be to use Arena simulation software to develop its gate security simulation. Figure 31 shows a block diagram of the gate security model that the TTG developed in Arena.

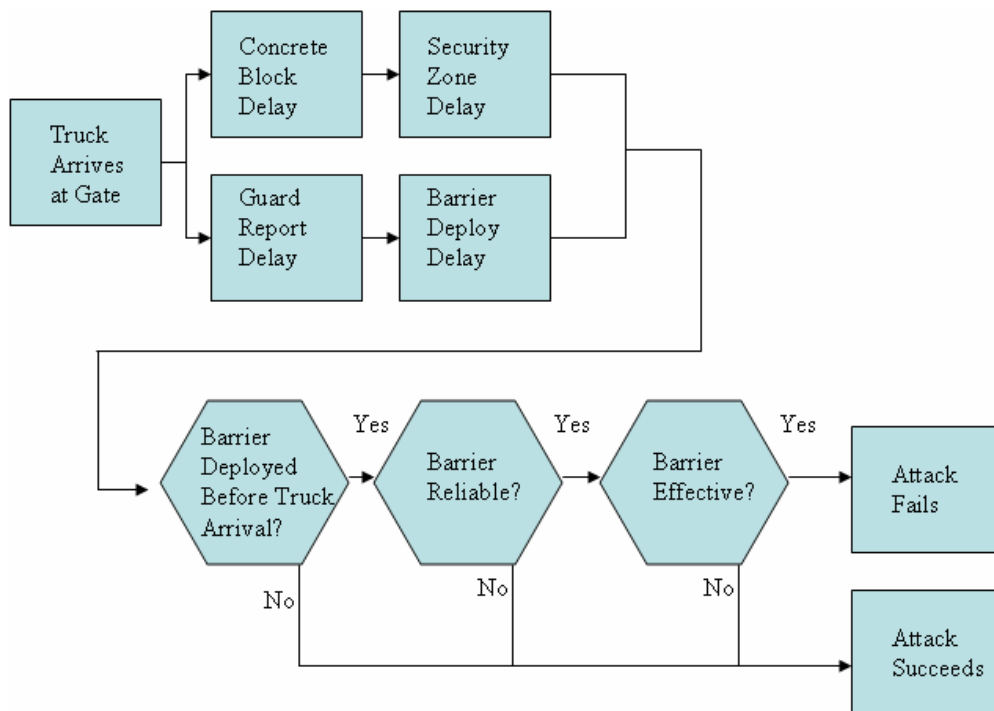


Figure 31. TTG Gate Security Model

The TTG model uses a series of delays and decision nodes to replicate gate operations when a vehicle attempts to drive past security without stopping. At the beginning of the model an “entity” is created to represent a terrorist truck arriving at the port’s gate. The entity is split into two identical entities to represent two parallel processes that occur when the truck drives past the gate. The first series is the truck’s actions, represented by a series of two delays. The first delay is the time that it takes the truck to negotiate any obstacles that may be in the truck’s path (concrete blocks), and the second delay is the time that it takes the truck to drive through the area between the guard house and the barrier (pop-up barrier, spike strips, or armed guard) that does not have obstacles in place. The second series is the defensive actions which are also represented by a series of two delays. The first delay is the time that it takes the guard to realize that there was a security breach, and to report the breach (hit the button to deploy the barriers, or call the armed guard on a radio), and the second delay is the time that it takes for the barrier to properly deploy (or prepare to fire in the case of the armed guard). It is important to note that all delays incorporated into the model are based on triangular distributions. After the identical entities have both proceeded through their respective delays, they are batched back into a single entity and then enter a decision node. The decision node is based on the delays that the entities experienced when they were split. If the defensive delays took longer than the truck delays, the attack succeeds, if not the defensive barrier had sufficient time to deploy and the entity that represents the truck moves on to the next decision node, reliability.

The reliability decision node takes into account the probability that the defensive measures will not always deploy when they receive the order to do so. In the case of the spike strips and pop-up barriers, if they are reliable they will pop-up and lock into position; in the case of the armed guard, he will successfully fire his weapon. If the barrier is not reliable, the attack succeeds. If it is reliable, the entity could proceed to the final decision node represented by effectiveness. The effectiveness decision node accounts for the fact that even if a barrier is successfully deployed before the truck arrives at it, the barrier still may not be successful at stopping the truck before it reaches the critical infrastructure that it intends to destroy. In our model reliability is a

percentage that we import into the model. The percentages that are imported into the model are primarily a function of speed, and in the case of the armed guard, it is also a function of the distance that the guard has to shoot at the approaching truck (200'+ is optimal). If the barrier is not effective, the attack succeeds; however, if it is effective, the attack fails and our system was effective. The primary MOE from this model is simply the number in the attack fails node/the number in the attack fails node plus the number in the attack succeeds node.

One of the most challenging aspects of modeling gate security was finding realistic values that could be used as inputs for each of the delay and decision nodes. A list of all of input values can be found in Appendix A, Table A2. It is important to note that all time delays are triangular distributions in seconds, all distances are in feet and all reliability and effectiveness is in percent true (95 percent reliability means that the barrier is reliable 95 percent of the time). All time delays for the truck are based on the TTG's calculations using the kinematics equations. The TTG assumed that all sets of concrete blocks would be 100 feet in total length and would force the truck to slow down to a maximum of 10 miles per hour in order to transverse the obstacles. The TTG assumed that the initial speed of the truck would be approximately 15 miles per hour at the gate when there were not concrete block present (before the gate) and that the truck would accelerate at a constant rate of .356 meters per second squared when it is on open road (no obstacles). The truck's acceleration was calculated based on a 400 horse power tuck with a gross total weight of 60,000 pounds. The calculated value was the multiplied by 80 percent and 120 percent to produce a triangular distribution that varied by 20 percent from the mean.

The time delays for the guards report time were based on a series of simple experiments conducted by the group. These experiments were used to determine the likely time that it would take the guard to hit a button on the wall that would activate the pop-up barrier or spike strips, or in the case of an armed guard to pick up his radio and hit the transmit button. The deployment times of the barriers were based off of the manufacturer's specifications, and in the case of the armed guard it was based off of a simple experiment performed by the TTG.

The TTG decided how velocity would affect the alternative's effectiveness. In the case of the pop-up barriers, the TTG determined that an increase in velocity would reduce the barriers effectiveness. According to several manufacturers of pop-up barriers, the most effective class of pop up barriers is certified for zero penetration by a 15,000 pound truck at 50 meters per second. Using the equation for momentum, the TTG converted this velocity to 12.5 miles per hour for a 60,000 pound truck. The effectiveness is set at 100 percent for all replications where the trucks terminal velocity is less than or equal to 12.5 miles per hour, and the TTG reduced the effectiveness as the trucks velocity increased. The TTG noted that the effectiveness of spike strips would be relatively low because even if they punctured the tires of the passing trucks, it is possible that the truck would be able to drive on flat tires and reach its target. The TTG determined that the faster the trucks velocity, the more effective the spike strips would be, as higher velocities would increase the chance that the terrorist would loose control of the truck and crash. The effectiveness of the armed guard was deemed to be best at medium distances because the truck would not be moving at great velocities and the guard would allow the guard a large enough time window to properly employ his weapon. As always the addition of an additional human to the loop reduces its effectiveness.

3. Analysis of Model Data

The data for the TTG's modeling is shown in Appendix B and is arranged into a bar graph in Figure 32. It is important to note that each data point is the average of 120 simulated days with 289 attempted attacks per day. When multiplied together TTG had a total of 34,680 attempted attacks averaged into every data point. In this section of writing, TTG created an abbreviation for each of its alternative configurations. For example, the abbreviation for a pop-up barrier with no concrete blocks at a distance of 100 feet from the guard house is PB-CB(N)-100. The first set of letters represents the alternative, the second set represents the concrete block configuration (or lack there of), and the number at the end represents the distance in feet between the guard house and the defensive barrier (or armed guard). Table 9 shows a list of the abbreviations used and their meanings.

Symbol	Representation
SQ	Status Quo
PB	Pop-Up Barrier
SS	Spike Strips
AG	Armed Guard
CB(N)	No Concrete Blocks
CB(G)	Concrete Blocks Before the Guard House
CB(B)	Concrete Blocks Before the Barrier

Table 9. TTG Model Abbreviations

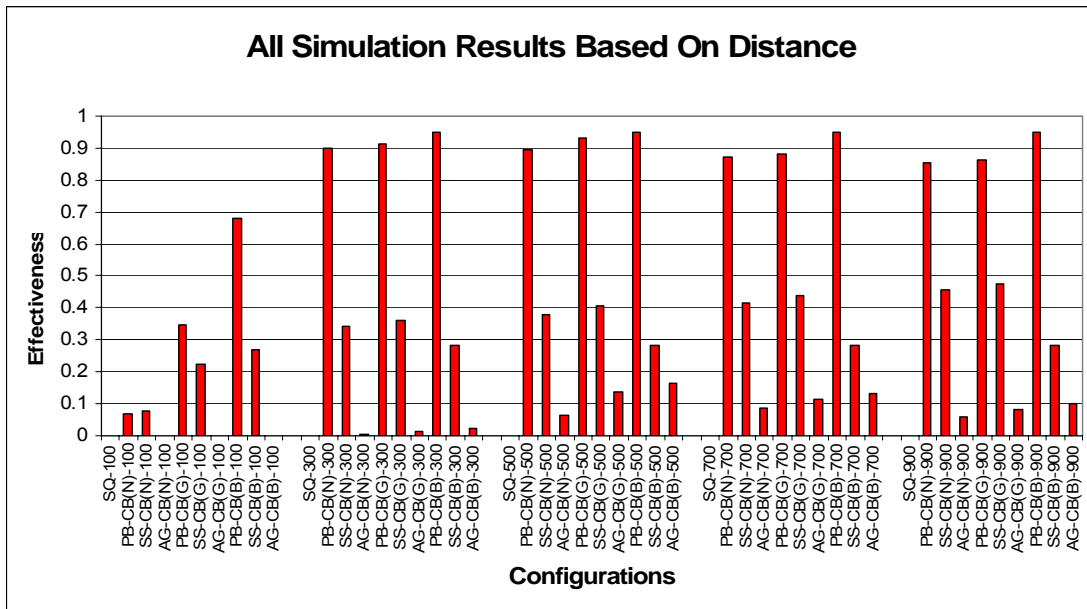


Figure 32. Simulation Results Based on Distance

The observations as can be seen from Figure 32 are:

- The Status Quo had an effectiveness of 0% for all distances because the Status Quo does not have a means to stop incoming vehicles.
- The performances of all configurations at the shortest distance of 100ft are the worst than that of all other distances for all alternatives. This is likely due to the short reaction time to deploy the barriers in order to stop the intrusions.
- At the longer distances of 500ft, 700ft and 900ft, the simulation results are relatively similar as the barriers had adequate time to deploy and the truck's speed at the barrier is the primary factor for the effectiveness of each alternative. For the simulations of deploying armed guards, there is an added variable of the engagement distances the armed guards have to

engage the truck, this was considered in the effectiveness node in the model.

It can also be noted from Figure 32 that there are four configurations, which tied for the highest effectiveness. They are PB-CB(B)-900, PB-CB(B)-700, PB-CB(B)-500 and PB-CB(B)-300. The conclusion that can be drawn from this result is that the deployment of Pop-up Barrier (PB) along with Concrete Blocks (CB) in front of the barrier to slow down the truck, and at a distance of at least 300 feet from the gate outperformed all the other configurations. A distance of at least 300 feet from the gate allows the pop-up barrier to have sufficient time to deploy and the concrete blocks in front of the barrier reduce the truck’s terminal speed. This causes the truck’s terminal speed while approaching the barrier to be identical regardless of distance between the guard house and barrier.

Figure 33 below shows all the simulation results based on the type of barriers deployed to stop the intrusion truck. This allowed us to analyze the performance of the different types of barriers in comparison to each other. Table 9 shows the abbreviations used and their meanings.

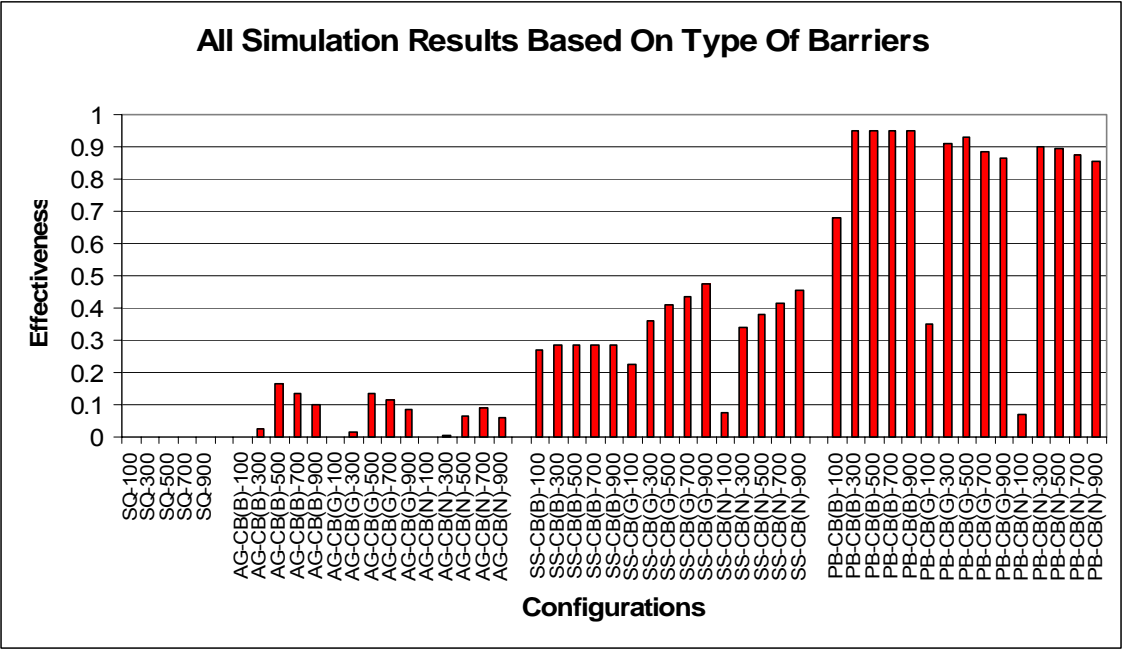


Figure 33. Simulation Results Based on Type of Barriers

The observations as can be seen from Figure 33 are:

- The deployment of pop-up barrier generally outperformed the other types of barriers (armed guards and spike-strips) used to stop the intrusion.
- The deployment of spike-strips is generally more effective than the deployment of armed guards. The addition of another human in the loop, and the natural hesitation to fire a weapon at a vehicle partially represents the poor effectiveness of the armed guard.

a. In Depth Analysis of Effectiveness of Armed Guard

The simulation results for the effectiveness of the armed guard in various configurations are shown in Figure 34. The general trend indicated that performance of an armed guard increases with an increase in range. The simulation has shown that an armed guard has a maximum effectiveness of only 16 percent at the range of 500 feet. Additionally, for ranges less than 300 feet, the various configurations of AG-CB(B) and AG-CB(G) performed with an effectiveness close to 0 percent. The armed guard was generally ineffective in stopping a moving truck regardless of barrier configuration. The performance of various configurations of the armed guard decrease from a high of 16 to 10 percent when the range is increased from 500 to 900 feet. This decline in effectiveness is likely due to the fact that a moving truck is more difficult for an armed guard to engage at higher velocities. Overall the simulations showed that an armed guard was generally ineffective at stopping a moving truck. Table 9 shows the abbreviations used and their meanings.

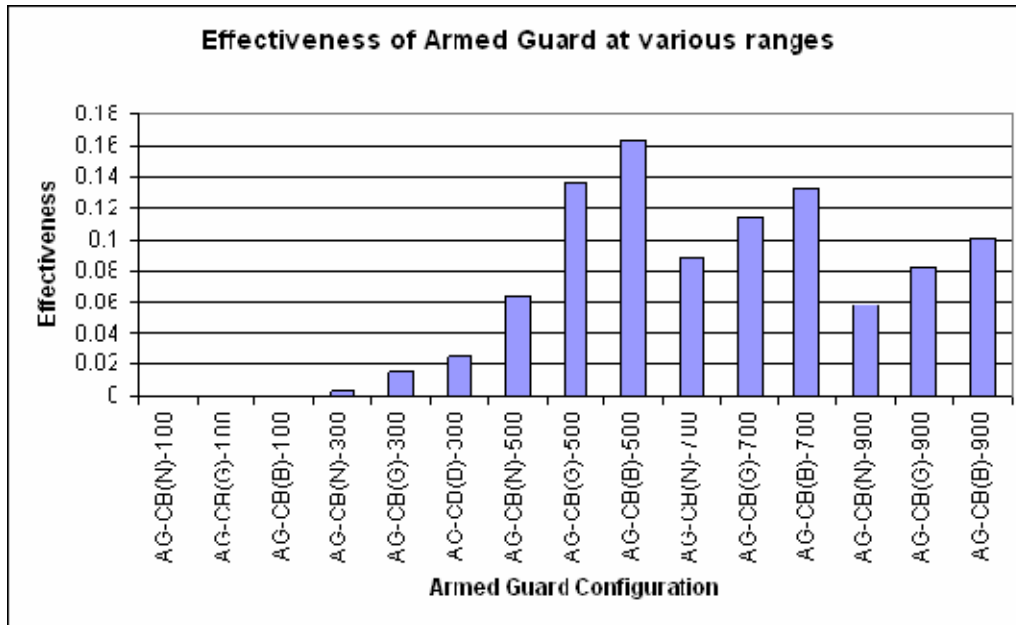


Figure 34. Effectiveness of Armed Guard Configurations at Various Ranges

Figure 35 shows the effectiveness of the armed guard with and without concrete blocks at various position, configurations and ranges. AG-CB(B) has the best overall performance at a distance of 500 feet. AG-CB(B) performance was better than AG-CB(G). Concrete blocks placed before the barrier slowed down the truck and give more time for the armed guard to react but the overall performance of armed guard with various configurations increases to a maximum at a distance of 500 feet and then reduces as the range continues to increase as a result of the truck's increasing velocity with distance. Table 9 shows the abbreviations used and their meanings.

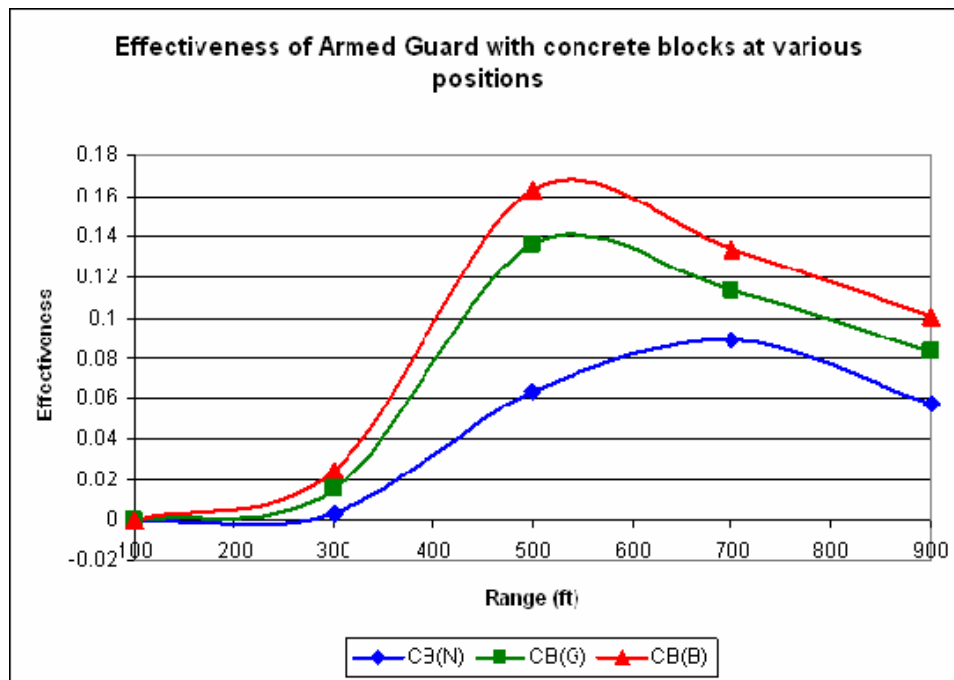


Figure 35. Effectiveness of Armed Guards and Concrete Blocks at Various Ranges

For all ranges, the AG-CB(G) and AG-CB(B) configurations appeared to be more effective (up to 3 to 4 percent) than the AG-CB(N) configurations since, with the concrete blocks positioned at the gate and barrier the slower velocity of the truck would permit the armed guard to have more reaction time.

A particularly noticeable trend was that the effectiveness with concrete blocks positioned at the barrier and gate increases sharply between the ranges of 300 and 500 feet (steep slope). The effectiveness of armed guard decreases when the range increased beyond 500 feet. It reduces at a rate of approximately 1.5 percent per 100 feet. With the concrete blocks positioned just before the armed guard, the speed of the truck was assured to be significantly lower than if the concrete blocks were not present. The performance of the armed guard was largely dependent on time period given for armed guard to react and truck velocity, its effectiveness was reduced as ranges increases (beyond 500 feet) due to the increase in the truck's velocity. This made it more difficult for armed guard to engage as physiology of human vision and response are factors needed to be considered.

The results of the relative effectiveness of concrete blocks when used with the armed guard are illustrated in Figure 36. The result was similar to Figure 35 as the best position of the concrete blocks was at the barrier and was most effective at a distance of 500 feet.

For ranges beyond 500 feet, the concrete blocks positioned at barrier provide almost constant three percent better performance in effectiveness than concrete block at gate. This performance gain could be attributed to the relative increase in reaction time caused when the trucks were forced to slow down by the concrete blocks. Table 9 shows the abbreviations used and their meanings.

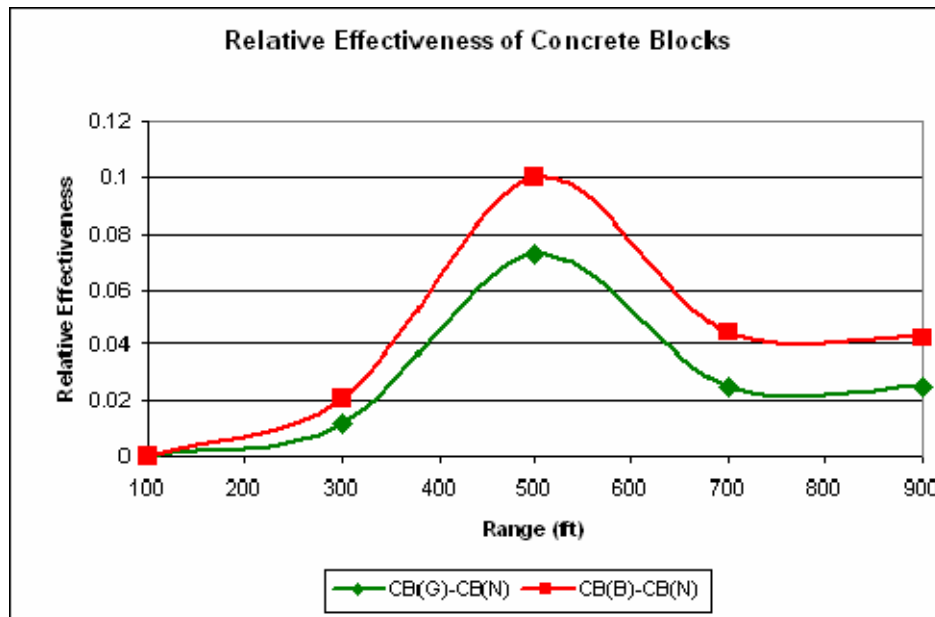


Figure 36. Relative Effectiveness of Concrete Blocks with Armed Guards

The results have shown that the armed guard was generally not an effective barrier for stopping a moving truck. The most effective configurations of the armed guard were AG-CB(B) at 500 feet. For ranges less than 300 feet, the effectiveness of an armed guard is near 0 percent. The outcome has shown that the concrete blocks enhanced the performance of an armed guard when deployed.

b. In Depth Analysis of Effectiveness of Spike Strips

The simulation results for the effectiveness of the spike strips in various configurations are shown in Figure 37. The results of the simulation show that, spike strips have a maximum effectiveness of 47 percent. The general trend indicated that the spike strips performed better at greater distances between the guardhouse and the barrier. Additionally, at ranges greater than 300 feet, the SS-CB(B) configuration appeared to be less effective than the SS-CB(N) and SS-CB(G) configurations. This is congruent with the fact that the damage caused by the spike strip on the truck is generally more severe when the truck approaches at a higher velocity, and at these velocities the driver was more likely to lose control of his truck when his tires were punctured. Consequently, the spike strip was relatively more effective when the truck approached at higher speeds. The best performing configurations were SS-CB(N)-900 and SS-CB(G)-900 with an effectiveness between 45 and 47 percent. Table 9 shows the abbreviations used and their meanings.

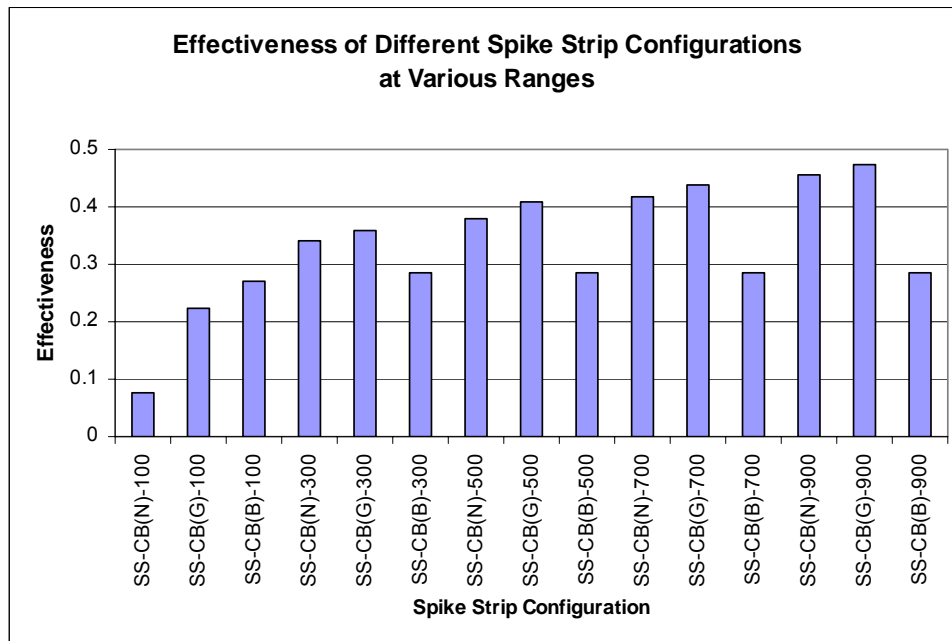


Figure 37. Effectiveness of Spike Strip Configurations at Various Ranges

Figure 38 shows the effectiveness of the spike strip with and without concrete blocks. Apart from the 100 feet configuration, the SS-CB(G) configuration

performed best, followed by the SS-CB(N) and SS-CB(B) configurations. In the 100 feet configuration, the SS-CB(B) configuration had the best performance as the concrete blocks stationed just before the barrier provided sufficient deployment time for the spike strip system. Table 9 shows the abbreviations used and their meanings.

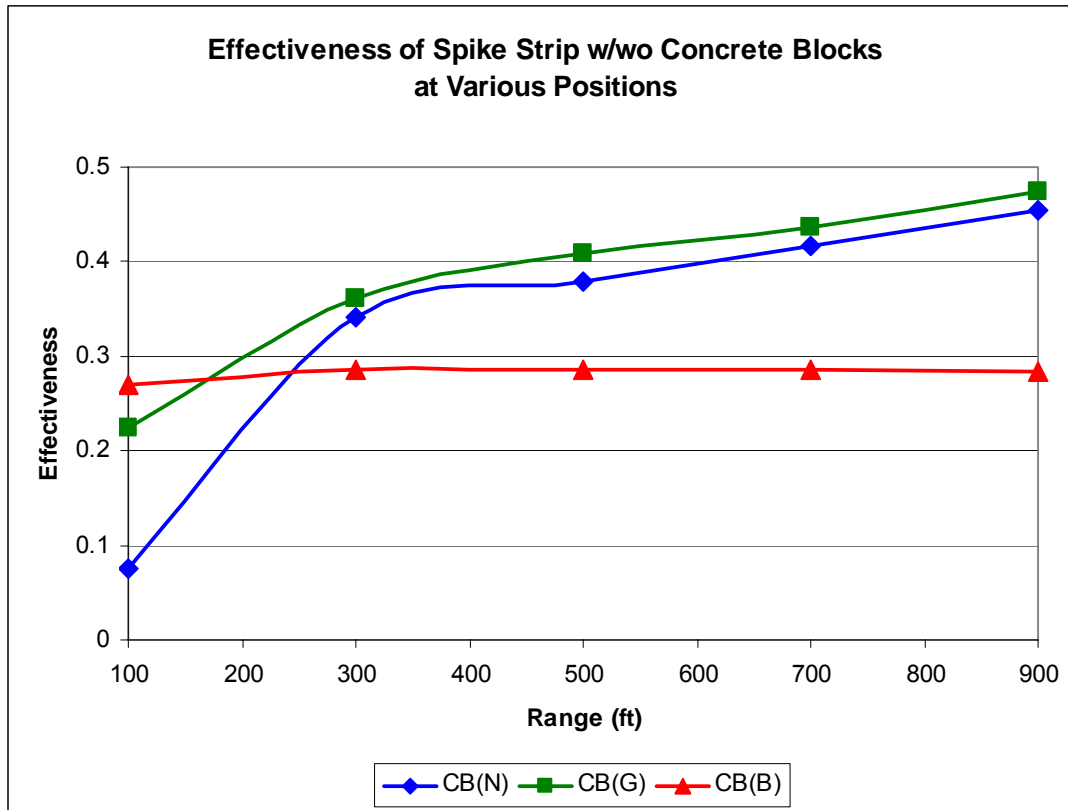


Figure 38. Effectiveness of Strike Strips and Concrete Blocks

For all ranges, the SS-CB(G) configurations was slightly more effective (about 2 percent) than the SS-CB(N) configurations. With the concrete blocks being positioned at the gate, the slower velocity of the truck would permit the guards to have more reaction time, but the truck would still maintain a relatively high speed at impact.

A particularly noticeable trend was that the effectiveness with concrete blocks positioned at the barrier location remained largely constant at approximately 28 percent. With the concrete blocks positioned just before the spike strip, the speed of the truck was assured to be significantly lower than if the concrete blocks were not present.

Since the performance of the spike strip was largely dependent on the truck's approach velocity, its effectiveness remained mostly constant for the SS-CB(B) configurations regardless of range.

The results of the relative effectiveness of the concrete blocks when used with the spike strip are as illustrated in Figure 39. A large increase in performance (about 15 to 20 percent) was observed only at the 100 feet range. At this close distance, the concrete blocks served to provide more time for the successful deployment of the spike strip system. Table 9 shows the abbreviations used and their meanings.

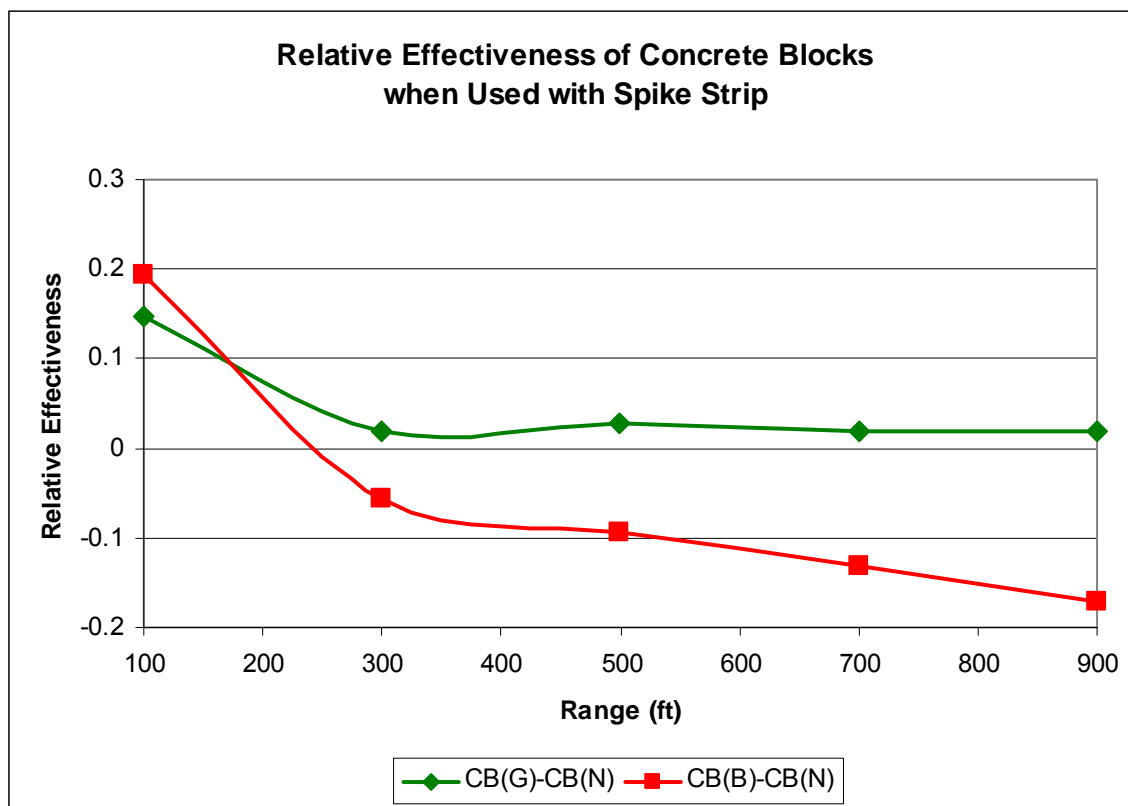


Figure 39. Relative Effectiveness of Concrete Blocks Using Spike Strips

However, at further ranges, the concrete blocks positioned at the gate seemed to provide only marginal increases (about 2 percent) in effectiveness. This performance gain could be attributed by the relative increase in available reaction time by the trucks being forced to slow down at the concrete blocks.

Furthermore, the concrete blocks appeared to degrade the effectiveness of the spike strip when they were positioned just before the spike strip. This was likely a result of the assessment that the spike strips are more effective when the truck approached at a higher velocity.

The results have shown that the spike strips were generally not an effective barrier for stopping trucks from reaching their destination within a port terminal. The most effective configurations of the spike strip were SS-CB(G) and they were valid for ranges greater than 100 feet. The outcomes have also shown that the concrete blocks generally provided minimal or negative performance gains when employed together with the spike strips even though there were some enhancements for the 100 foot configurations.

c. In Depth Analysis of Effectiveness of Pop-up Barriers

The results of the simulation for the effectiveness of the various configurations of the pop-up barriers are shown in Figure 40. In general, configurations that included concrete blocks performed better than those without concrete blocks. The results indicated that there might be an optimal range beyond which the effectiveness either stayed constant or decrease. The configurations that showed the best performance were the PB-CB(B) that is installed at distances of more than 300 feet from the gate. These configurations resulted in a system effectiveness of approximately 95 percent. Table 9 shows the abbreviations used and their meanings.

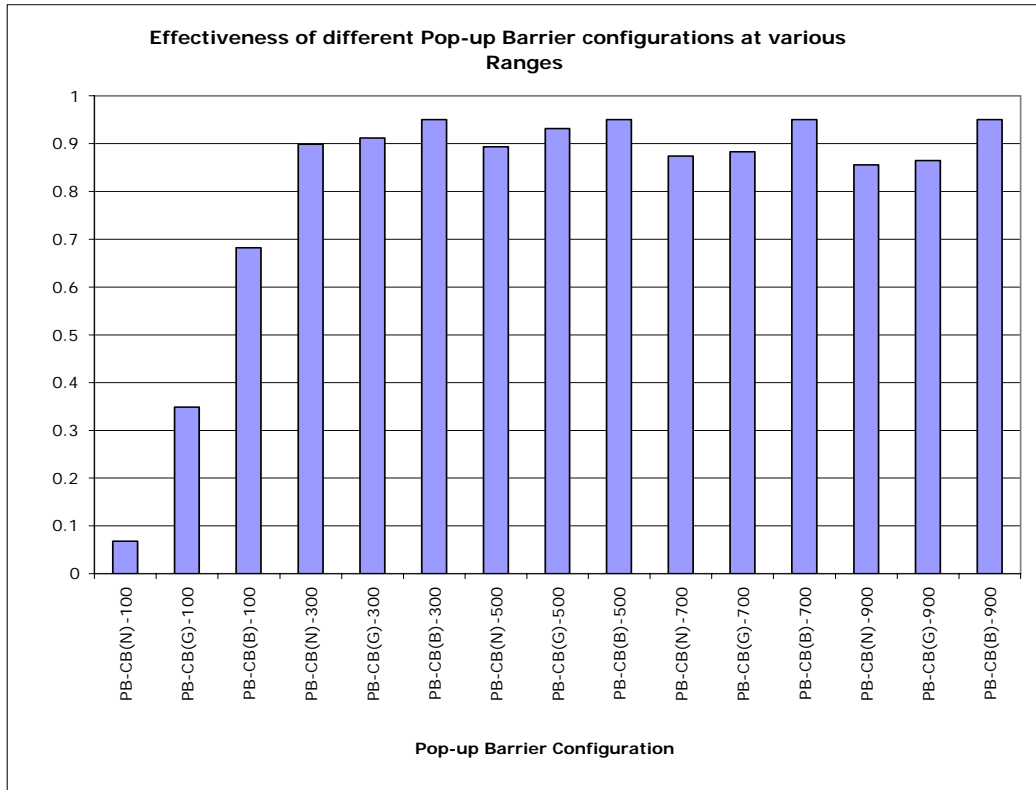


Figure 40. Effectiveness of Different Configurations of Pop-up Barriers

At all ranges, the PB-CB(B) performed better than both the PB-CB(G) and PB-CB(N) as shown in Figure 41. Beyond 300 feet, PB-CB(B)'s effectiveness was relatively constant; increasing the distance between the gate and the barrier beyond 300 ft did not increase the effectiveness of PB-CB(B). At 100 feet, the effectiveness dropped to 68 percent, but was still significantly higher than that of PB-CB(N) at 7 percent. Additional simulation runs at 200 feet (not showed in the figures) showed that in fact the effectiveness of PB-CB(B) had reached 90 percent at 200 feet. For PB-CB(B), the range of 200 feet combined with the concrete blocks in front of the barrier provided sufficient time for the barrier to be completely deployed. This combination was the most effective alternative set for all distances. Table 9 shows the abbreviations used and their meanings.

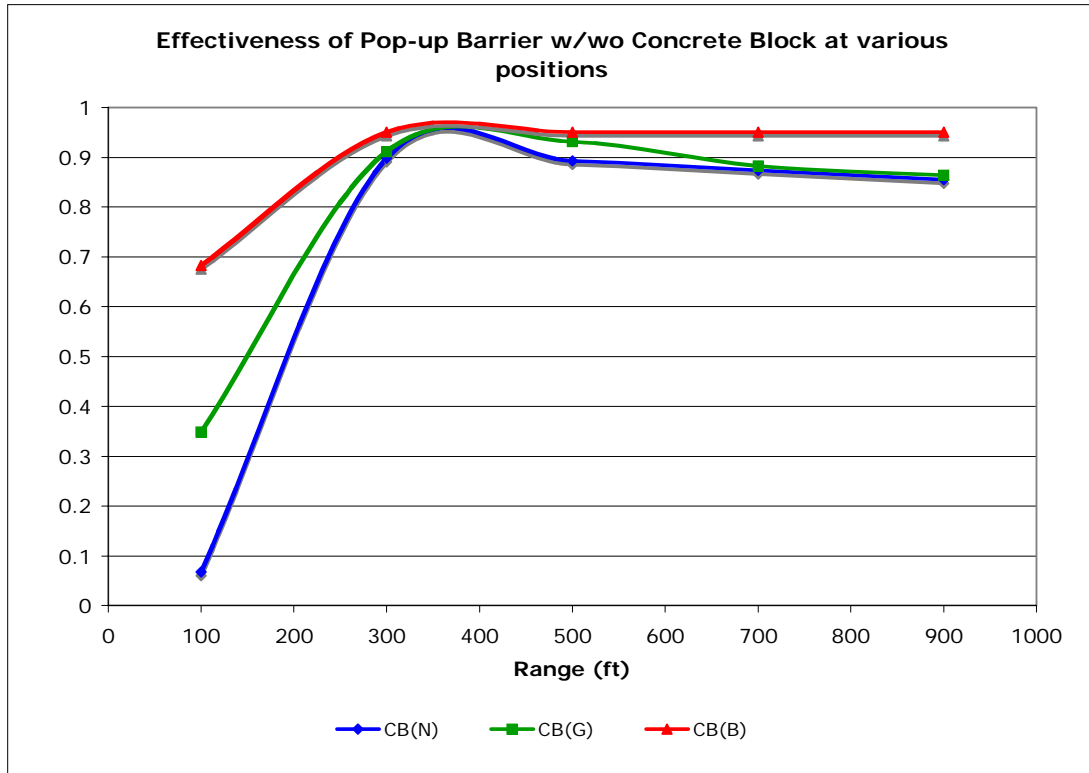


Figure 41. Effectiveness of Pop-up Barriers and Concrete Blocks

PB-CB(G) performed better than PB-CB(N) at range of 100 feet but has similar performance beyond 500 feet. At short range, the concrete barrier at the gate provided more time for the barrier to deploy, while at longer ranges this difference became insignificant. Figure 42 shows the absolute difference in effectiveness between configurations with concrete blocks and those without concrete blocks. Table 9 shows the abbreviations used and their meanings.

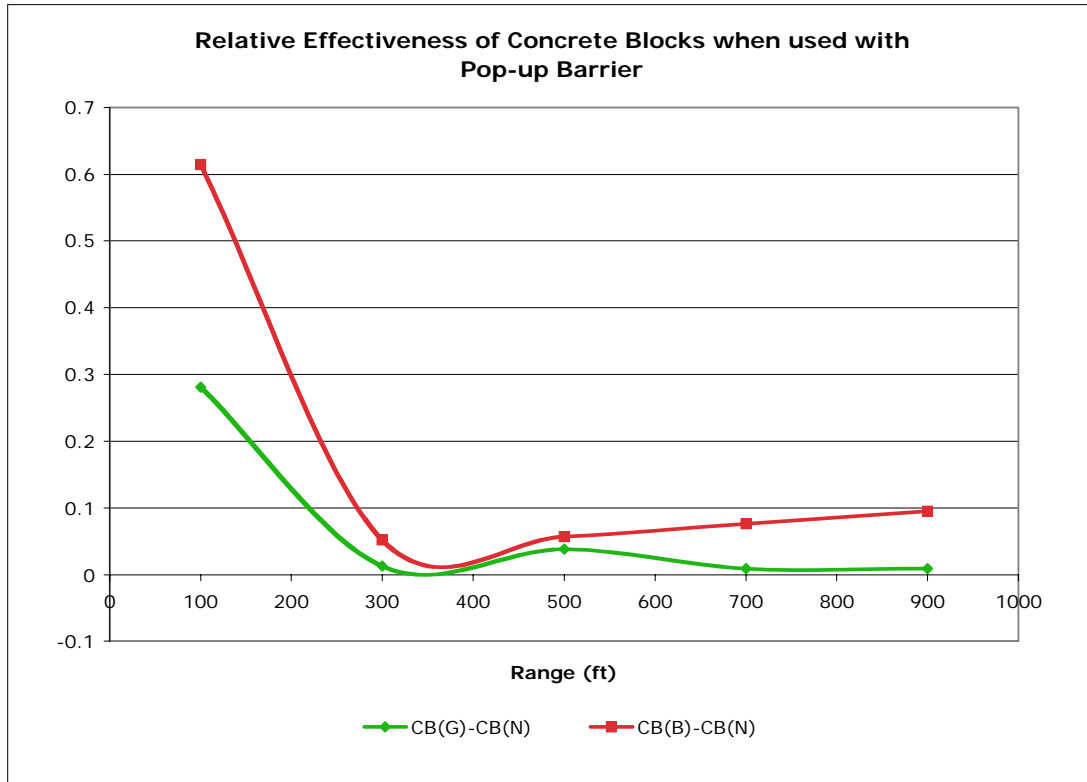


Figure 42. Relative Effectiveness of Concrete Blocks with Pop-up Barriers

The most effective configuration of pop-up barrier is the PB-CB(B). This configuration was most optimal when installed at approximately 300 feet or more from the activation point (gate). The concrete blocks enhanced the performance of the pop-up barrier at all ranges and were more significant at shorter distances. Concrete blocks were more effective when placed just in front of the pop-up barrier than at the activation point (gate).

d. Data Analysis Conclusions

In the scenario where terrorist plans a truck laden with explosives and attempts to drive through the gate security measures, the TTG's analysis indicates that the most effective implementation against such terrorist attacks is the PB-CB(B)-300+ configuration. The current analysis has not taken life-cycle implementation cost into consideration. Hence, later in the writing, the TTG will evaluate the cost and benefit by

considering the life-cycle implementation cost for a complete assessment on the practicality of recommended implementation.

4. Cost Estimation

The TTG conducted cost estimations of the perimeter defense alternatives to enable it to later conduct a cost benefit analysis. The cost benefit analysis shows the stakeholders the amount of anticipated performance that could be achieved for a given cost and which alternatives are dominated by others. It identifies the alternatives that both cost more and perform less than at least one of the other alternatives, it is never economically sound to implement an alternative that is dominated by a different alternative. The TTG cost estimation included not only the alternatives considered in the modeling and analysis phase of the project, but it also included a cost estimation on hardening a ports perimeter fence. As presented earlier in the paper, it is illogical to implement gate defenses before hardening the perimeter fence, as doing so would simply lead the terrorist to crash through the fence and avoid the gate security altogether. The TTG did not include cost estimation for hardening the critical infrastructures inside the port. As previously mentioned in this paper, the high economic value of land inside a port terminal and the relatively larger destructive radius of a large blast weapon would likely make the opportunity cost of hardening the port's critical infrastructure infeasible.

a. Cost Estimate for Hardening Perimeter Fencing

The TTG narrowed the alternatives for hardening a port's perimeter fence down to the two most likely choices. The port would likely build a concrete or brick fence or align concrete blocks at the base of the already existing chain link fence.

For the purpose of this study, all costs are in 2007 U.S. Dollars (USD). Based on market survey, the cost for erecting a concrete perimeter fence ranges from \$100 to \$400 per foot, depending on the height and material used. The TTG used the average of \$250 per foot for its cost estimation. It would cost the port approximately \$75,000 per 100 yards of perimeter fence to implement this type of a fence.

Implementing steel reinforced concrete blocks as a means to harden the port's perimeter fence would cost the port approximately \$100 per eight foot concrete block [41]. The implementation of a continuous barrier of concrete blocks at the base of the preexisting chain link fence it would cost the port approximately \$3,750 per 100 yards of perimeter fence.

The Port of Oakland has approximately 6,000 yards of perimeter fence, of which approximately 50 percent is unhardened. To harden the remaining 3,000 yards of perimeter fence would cost the Port of Oakland approximately \$2,250,000 to implement a concrete fence, or \$112,500 for concrete blocks. Given the large price disparity it is expected that most ports would choose to implement steel reinforced concrete blocks in order to harden their existing perimeter fencing.

The following cost estimations were conducted on the alternatives that were previously explored during the modeling and analysis phase of this project. The cost estimation for each alternative was later compiled and examined in a cost benefit analysis.

b. Cost Estimate for Armed Guard

Port security was viewed as important for port operators but it was not the primary business for any port operator; instead the terminal operator is in business to make money. The TTG determined that it was most effective and efficient to outsource the port security services to a professional security agency for better resources management and for long term sustainability. Outsourcing of security services allowed port operators to concentrate on their primary business. Outsourcing of the security services does not imply that the port operator has no obligation to the security of the port, but instead that he chose to utilize an outside company with security expertise and professional training.

Based on market survey, the hourly rate for a well trained armed security guard services was between \$14 to \$30, depending on the size of the contract and the services that the armed guard was required to perform. Additional cost would be imposed if the armed guard was involved in patrol or investigation services, but this cost would

not be imposed on TTG's proposed armed guard alternative, as the guard would be stationary.

For the purpose of this report, the TTG utilized an hourly rate of \$17.44 per armed guard [42]. This is a term contract rate for armed security guard services awarded by the state of New Jersey Treasury Purchasing Department for contract number 59555 between 2004 and 2007. TTG assumed that each port terminal conducted gate operations for 40 hours per week and required a single armed guard during normal gate operations. The annual cost to the terminal operator for adding a single armed guard for an 8 hour shift would be approximately \$36,275.

c. Cost Estimate for Spike Strips

The material cost of a spike strip traffic controller covering a single 12 ft lane is estimated to be \$30,000 and the installation cost is expected to be \$5,000. The annual operating and maintenance cost for a system is about eight percent of the total procurement cost [43]. The expected life span for such a system is about 10 years.

The TTG determined that each terminal required a minimum of two lanes of spike strips, as during maintenance periods, this would allow one lane to operate while the spike strip system in the other lane was maintained. For a system of spike strips to cover two lanes, the estimated cost for material and installation is approximately \$70,000. Additionally, the operating and maintenance cost is approximately \$5,600 per year. Table 10 depicts the cost estimates for employing spike strips.

Item	Description	Unit Cost	Quantity	Cost
Spike Strip	A system of spike strip covering a 12 ft lane.	30,000	2	60,000
	Installation	5,000	2	10,000

Table 10. Cost Estimation Table for Spike Strips

Assuming that the system had a life span of 10 years and the system was not financed, but instead purchased outright, the system had a total average annual system cost of \$12,600 for two lanes. If the port terminal instead chose to finance the spike strip system over the expected life span of 10 years at an annual interest rate of

seven percent with no down payment, the annual payments for the system would be \$9,966. If we then consider the operation and support costs for the system, we arrive at a total annual system cost of \$15,566.

d. Cost Estimate for Pop-Up Barrier

The material cost of a pop-up vehicle barrier with DOS K-12/L-3 rating [44], ranges between \$33,000 to \$55,000 for a system that covers a single 12 feet lane [43]. The installation cost for such a system is an addition of about 90-95 percent of the material cost. The annual operating and maintenance cost for a system is about eight percent of the total procurement cost. The expected life span of such a system is 10-15 years.

Assuming that the system has an acquisition and installation price of \$97,500 per lane, the cost to acquire and install two sets of pop up barriers is approximately \$195,000. In addition, the annual operating and maintenance cost for the two lanes is approximately \$15,600 per year. Table 11 depicts the cost estimates for employing pop-up barriers.

Item	Description	Unit Cost	Quantity	Cost
Pop-up Barrier	A system of DOS K-12/L-3 rating covering a 12 ft lane.	50,000	2	100,000
	Installation	95% of material cost	2	95,000

Table 11. Cost Estimation Table for Pop-Up Barriers

Assuming that the system had a life span of 15 years and the system was not financed, but instead purchased outright, the system had a total average annual system cost of \$28,600 for two lanes. If the port terminal instead chose to finance the spike strip system over the expect life span of 15 years at an annual interest rate of seven percent with no down payment, the annual payments for the system would be \$21,410. If we then consider the operation and support costs for the system, we arrive at a total annual system cost of \$37,010.

In addition to the cost estimation of the three alternatives listed above, TTG conducted a cost estimation for the implementation of concrete blocks. The purpose the concrete blocks was to force inbound vehicles to reduce their speed as described in the alternatives generation and modeling and analysis portions of this paper. The implementation of concrete blocks is used in conjunction with the other alternatives to increase their overall performance and the cost of concrete bocks needed to be considered for each alternative where they increased the overall system performance.

e. Cost Estimate for Concrete Blocks

The usage of concrete blocks has been analyzed to be able to enhance the effectiveness of protective measures against the “Truck runs gate scenario”. The implementation is possible on a single lane as indicated in Figure 43.

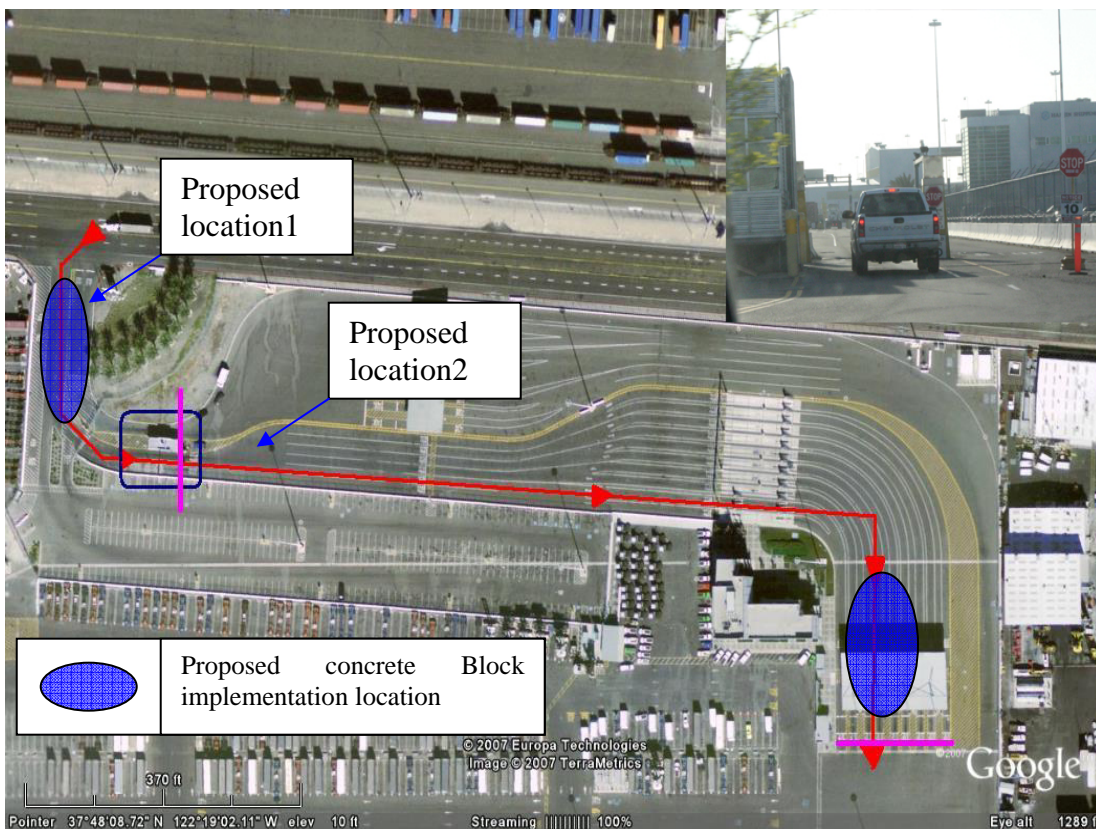


Figure 43. Concrete Block Implementation

To effectively use the concrete block to limit the speed of potential threats, an implementation of four layers of concrete blocks with 40 feet spacing would be sufficient to effectively limit the vehicle speed to 20 miles per hour over an implementation distance of 120 feet as illustrated in Figure 44 [45].

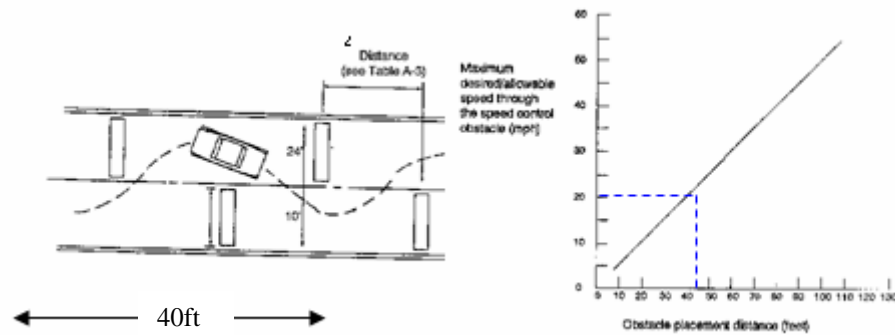


Figure 44. Concrete Block Effective Placement for 20 MPH Speed Limit

The material cost of a basic concrete block is approximately \$100 each [41]. While installation cost for four blocks was expected to be approximately \$500. Since its implementation is expected to be permanent, the operating cost is expected to be negligible. Maintenance cost for the concrete block over a life span of 10 years is also expected to be insignificant. Table 12 depicts the cost estimates for employing concrete blocks.

Item	Description	Unit Cost	Quantity	Cost
Concrete Blocks	Concrete Blocks	100	4	400
	Installation	500	1	500

Table 12. Cost Estimation Table for Concrete Blocks

The total cost for implementing a set of concrete blocks to reduce the speed of incoming traffic was expected to be approximately \$900. The average annual cost of implementing concrete block over their expected 10 year life span was \$90. This meant that \$90 needed to be added to the annual cost of each of the alternatives, if the use of concrete blocks was considered advantageous.

5. Cost Benefit Analysis

A cost benefit analysis is an analysis between the modeled alternatives that compare the cost and effectiveness. A complete cost benefit analysis will answer the following questions for the stakeholder: What level of effectiveness can be achieved for a given cost? What is the cost of a given level of effectiveness? And which alternatives are dominated and should not be considered? The TTG conducted a cost benefit analysis on the alternatives considered during the modeling and analysis phase of this project. Appendix D, Table D1 contains a table of the cost and effectiveness of each alternative configuration. Figure 45 shows a cost vs. effectiveness graph of the most effective combination of all four alternatives. It is important to note that the cost is the average annual total system cost and both the spike strips and pop-up barrier costs are the costs if the barrier was financed, as stated in the previous section.

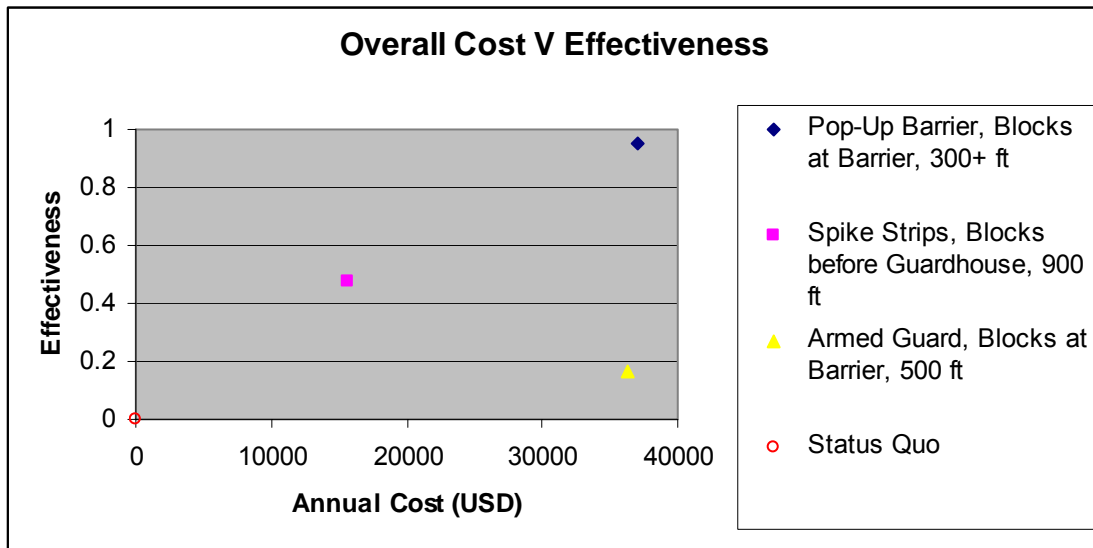


Figure 45. Cost vs Effectiveness of Alternatives

The efficient frontier is composed of the set of non dominated alternatives, which means that they have the lowest cost for the level of performance that they provide. From Figure 45, it is clear that an efficiency frontier exists among the alternatives. The efficiency frontier for gate security include: The status quo, spike strips, and pop up barriers. The efficiency frontier does not include the implementation of an armed guard

because the implementation of spike strips both costs less and performs better than that of an armed guard. The implementation of an armed guard is clearly dominated by the implementation of spike strips.

Appendix D, Figures D1 through D4 presents cost versus effectiveness graphs for given ranges (700, 500, 300, and 100 feet). This presentation of cost versus effectiveness is useful when the port terminal is physically limited by the space that can be placed between the guardhouse and the barrier. All three graphs in Appendix D have the same general shape, efficiency frontier, and dominance as Figure 45. The important takeaways from the cost benefit analysis are that an armed guard should never be implemented in an attempt to improve gate security, as the port achieves greater performance at a lower cost by instead implementing spike strips, and although the status quo is on the efficiency frontier, its is completely ineffective at stopping a truck from gaining access to the port terminal. If port management desires to improve its gate security, they should choose to implement either spike strips, or pop-up barriers. The spike strips cost less than pop-up barriers, but pop-up barriers perform better than spike strips, it is up to the stake holder to determine which system is best for their unique needs.

III. REGIONAL SEABORNE THREATS GROUP

A. PROBLEM DEFINITION

1. Needs Analysis

Prior to the September 11th 2001, the various security agencies in Singapore already operated a well-coordinated and thorough security framework. Following the September 11th attack, Singapore had intensified its port security measures. These measures were aimed to safeguard sensitive installations such as major oil, chemical terminals, cruise, and ferry terminals.

The Port of Singapore and major waterways were under constant surveillance. Key areas within the Port of Singapore such as waters around chemical and off-shore oil terminals were declared as restricted areas and small craft entering these areas were to seek written approval from the MPA [8].

The MPA closely monitors the movement of sensitive vessels including liquefied petroleum gas (LPG), liquefied natural gas (LNG), chemical tankers, oil tankers and passenger ships. The relevant security agencies conduct sea patrols to ensure the various vessels were in compliance with port security restrictions. Regional ferries, Indonesian Barter Trade Craft and pleasure craft had their routes revised to prevent such craft from passing closely to sensitive areas and vessels in port [8].

Sea entry checkpoints were strengthened. Security at sea entry checkpoints was tightened to prevent entry of undesirable persons and dangerous weapons. Persons entering or leaving Singapore by sea, including passengers and crew members going ashore were to be subjected to a face-to-face check by ICA (Immigration and Checkpoints Authority) at designated landing points. All arriving vessels were to anchor at designated immigration anchorages, where the ICA's officers boards and conduct face-to-face checks.

Singapore adopted the ISPS (International Shipping and Port Facility Security) since 1st July 2004. Singapore was one of the first countries in the world to fully comply with the IMO requirements. There are 1270 Singapore registered ships and 118 port

facilities compliant with the ISPS code. Of the 118 port facilities, 25 of them serve ships of less than 500 gross tons (GT) and need not comply with the code but chose to do so as they felt that the ships that they interfaced with ventured outside the port waters.

In compliance with the ISPS code, Singapore had executed 3 major maritime security exercises at sea involving all the security agencies, operators of sensitive installations (Shell and ExxonMobil) and sensitive vessels (LPG carriers) since 2004. Random audits were also conducted with security organizations to ensure that security procedures are adhered to at port facilities and on ships.

Three security levels were adopted in accordance with the ISPS Code. The three levels are as follows:

- Security Level 1- normal; the level at which ships and port facilities normally operate. It means the level for which minimum appropriate protective security measures shall be maintained at all times.
- Security Level 2- heightened; the level applying for as long as there is a heightened risk of a security incident. It means the level for which additional protective measures shall be maintained for a period of time as a result of a security incident.
- Security Level 3- exceptional; the level applying for the period of time when there is a probable or imminent risk of a security incident. It means the level for which further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target.

The security level would be set by MPA with the aid of the intelligence agencies and the Ministry of Transport. Presently, the Port of Singapore is at Security Level 1.

MPA also set up a 24-hour Maritime Security Unit to monitor and receive all ISPS ships' submissions of security-related information prior to the entry of the ship into port. The information known as Pre-Arrival Notification of Security (PANS) is to be submitted at least 24 hours before the ship's arrival in Singapore. This information includes the last ten ports that the ship has called and any special security measures put in these ports.

ISPS ships are to be provided with a ship security alert system (SSAS). The SSAS when activated will transmit a ship-to-shore security alert to the administration

identifying the ship, its location and indicating that the ship is under threat. All Singapore-registered ships will send the security alerts to the MPA regardless of their locations. The MPA has a standard operating procedure with the RSN (Republic of Singapore Navy) and PCG (Police Coast Guard) to handle ship security alerts.

For non-compliant ISPS ships, control measures that were put in place are:

- Denying entry
- Inspection of the ship
- Delaying the ship
- Detention of the ship
- Restriction of operations
- Movement within the port
- Expulsion of the ship from port

The ISPS code largely focuses on commercial facilities and the larger vessels. Therefore, smaller vessels (<500 GT) engaged on international voyages are not compelled to comply with the ISPS Code. However, these small vessels are also vulnerable to security threats and could be used as weapons like vessels that require compliance with the ISPS Code. The USS COLE attack in Yemen in October 2000 and the French Tanker LIMBURG incident in October 2002 are well known.

The port remains vulnerable to security threats from both arriving non-ISPS compliant vessels and vessels from non-ISPS compliant ports. Control measures are put into place by MPA to deal with vessels coming from non-ISPS compliant ports. Additional measures to the ISPS Code were implemented to safeguard the ships and port facilities to further enhance maritime security within port waters. The developed measures were:

- Guidance for establishing security measures when vessels call at non-ISPS compliant ports
- Ship Self-Security Assessment Checklist
- Harbor Craft Security Code
- Pleasure Craft Security Code
- Harbor Craft Transponder System

Not all the port facilities in the world are ISPS compliant, guidance is provided to ISPS compliant ships calling from non-ISPS compliant ports. The ships are to take the

directed additional measures while in a non-complaint port. Examples of such measures are:

- Restricting access to the ship
- Deployment of security guards at gangway
- Restricting visitors from the ship
- Securing accommodations
- Checking for stowaways in the engine room and store rooms
- Checking packages and baggage brought onto the ship

The U.S. Coast Guard had recently asked to post the guidance on their website, as a means of exchanging experiences and sharing best practices to enhance port security.

MPA requires the small sea-going vessels of under 500 GT calling at the port to complete a SSSA prior to port entry. The checklist is to be kept on board for verification by the security agencies or port officials.

All harbor craft (<500 GT) have to comply with the Harbor Craft Security Code (HSCC) and the security log. The HCSC encompasses simple and practical actions taken by harbor craft masters to protect the crewmembers and the craft so as to mitigate the vulnerability to security incidents on board. The HCSC contains the key security measures to ensure the security readiness of the harbor craft while operating in the port waters.

MPA developed a Pleasure Craft Security Code (PCSC) to further enhance security in the port waters. The Code is user-friendly and was developed in consultation with the pleasure craft community. The PCSC provided security guidance to the pleasure craft community and focus on four key areas:

- Need for preparedness
- Vigilance when navigating
- Maintaining an observant posture
- Being proactive in reporting to the appropriate authorities

Harbor craft less than 300 gross tons and not engaged on international voyages, do not come under the Safety of Life at Sea (SOLAS) Regulations and hence are not required to carry the Automatic Identification System (AIS) transponders. Recognizing the potential threat, the MPA and the security agencies, developed a vessel tracking system known as the Harbor Craft Transponder System (HARTS) as an added defense

against potential attacks by small craft. All the 2,800 MPA-licensed powered harbor and pleasure craft were fitted with the HARTS transponders. The system has been operational since 1 January 2007.

To prevent unauthorized use, a special coded identity of each transponder ensures that the transponder could only operate on the harbor craft on which it was installed. The coded identity must match that of the mounting bracket. This security feature ensures the transponder will not work if used on another craft. In the event of a security breach, an alert would be sent to the control center operator.

Every transponder is equipped with a panic button. The panic button allows the craft owner/master to alert the MPA in the event of distress or a security threat. After activating the panic button, an alert message containing the identity, position and time is sent to the control center operator. This function is similar to the IMO Ship Security Alert System for ocean-going vessels.

MPA has introduced a new licensing scheme for regional ferry operators. The new licensing regime formalizes the need for compliance to safety and security measures. This is important since ferry services are a popular mode of transport for traveling between regional destinations.

Since 1 January 2005, companies that operate regional ferry services are required to obtain a license in order to provide such services in Singapore. This licensing scheme is part of ongoing efforts to safeguard the security of the ferries and passengers.

For the purposes of protecting the port and vessels from security threats, all vessels entering or leaving the port of Singapore may be boarded by a team of police officers or authorized representatives of the Port Master. The teams board arrival vessels with pilots at the pilot boarding grounds or for departing vessels, the team would board with the pilots at anchorages or berths, as far as practicable.

MPA adopted a multi-agency approach in ensuring maritime security and works closely with the Home Teams (Homeland Security) and the RSN. Various task forces, committees, and working groups have been established to examine the different aspects of maritime security. The smooth implementation of the various security measures in the

port includes conducting security exercises, which have been possible only because of close-operation between the security agencies and the stakeholders like the port facilities' operators and the ship-owners.

For the global approach, MPA participates in various regional and international forums as well as correspondence groups initiated at these forums to share expertise and to exchange information among the member countries.

a. System Decomposition

For regional port security which is deemed waterside standoff, this model represents what the system needs to accomplish to achieve its purpose. The ability to maintain waterside security is dependent upon four areas. The sub-elements for each area are elements that provide the larger component to exist thereby providing the ability for waterside standoff which reflects regional port security, shown in Figure 46.

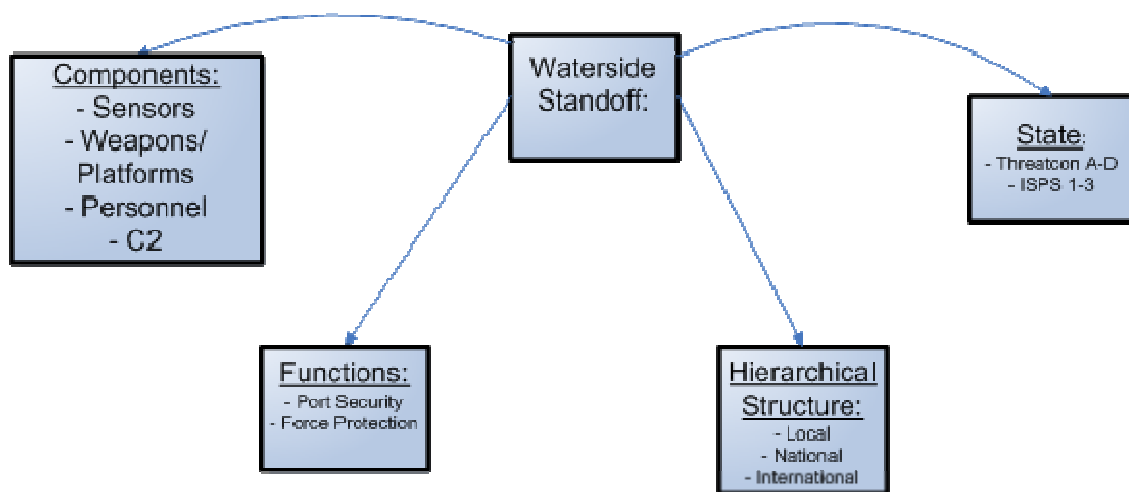


Figure 46. RSTG System Decomposition

b. Stakeholder Analysis

The primary stakeholders were subdivided into two groups: authorities/agency and users. In each of these groups, the concern about force protection and port security is a relevant issue. Each of the groups envisions the issue in somewhat of a different aspect; therefore, the need to resolve the issue is important. When dealing

with the regional seaborne aspect of port security, from the pier to the port boundary, the threats may be small boats, large ships, swimmers, and autonomous underwater vehicles (AUVs). From a regional perspective, the ports of Oakland and Singapore were examined. Each of these ports envisions regional aspect of port security in different ways yet there were many similarities.

The Singapore Port Authorities have the following key concerns:

There is a need to balance the quick flow of trade and commerce against the need to enforce and implement the various security measures. While the fact remains the security is paramount to safeguard the interests of the commercial trade, the implementation must not be too burdensome to the users of the port. Also, any implemented security measures must not adversely increase the time the ships use Singapore as a port-of-call.

Singapore is only one of the several littoral states along the Straits of Malacca (the others being Malaysia and Indonesia), meaning that international cooperation is required for any successful response to the prevailing maritime security threats. This is due to the fact that the identified threats are primarily trans-national. Action from the Singapore Port Authorities alone will not be sufficient to totally negate these threats. The fact that these threats are not concerned with territorial boundaries means that international cooperation is paramount to the success of ensuring maritime security in the region. This co-operation is, however, sometimes affected by political relations between the states, which the port authorities cannot control. While cooperation between the states in recent years has improved significantly, more can still be done.

The Oakland Port Authorities have the following concerns:

Like that of the Singapore, the need to implement port security measures are required post 9/11. The one operation that cannot be severely affected when a new port security measure is implemented is the flow of commerce. This aspect is a common thread of high importance. In the eyes of all parties, time is money to the commercial side of the house. From the military's view, safety and operational readiness are the primary issues for ships overseas in foreign ports. What the Oakland Authorities desire is

a feasible alternative that will suit the port facility. When the cost of security is increased, the expense is paid by the vessel owners, ultimately increasing the price of goods to the consumer.

With the port of Oakland, the right of freedom of navigation is an issue. In the cases of naval installations and oil refineries, there are established security zones which more readily provides intent for penetrating personnel/watercraft. For the Port of Oakland, this is not the case; the ability of the port to delineate a security zone around the port is infeasible. The number of vessels coming into and out of the port and the required manpower to support this initiative is too costly. The number of recreational vessels in and around the Port of Oakland varies. The implementation of a security zone would cause a political backlash. Initiating this security measure requires legislation and enforcement by the DHS agencies.

c. Input-Output Model

The purpose of the input-output model is to help devise a system providing security of the waterside portion of the pier. This model examines the general commercial ports as well as the military ports. The system will examine an active system that will provide pier protective measures. In this model, two aspects are observed and contribute to the system which will result in an intended affect as well as by-products of the system. Controllable elements are self explanatory with the exception of the types of vessel and port reaction to the threat. Types of vessels refer to the large ships that are on a predetermined schedule and are designated to moor to certain piers. Port reaction to the threat is the time of response to address a threat as well as an elevation in threat condition. Uncontrollable elements are those aspects that have a lot of variability and whose results are undeterminable. For the uncontrollable input, enemy strike refers to who, what, where, when and why. From the interaction with the system, positive and negative intended actions as well as by-products are the outputs. These inputs are required by the system to function and to address the force protection and port security issues. Figure 47 depicts the RSTG input-output model.

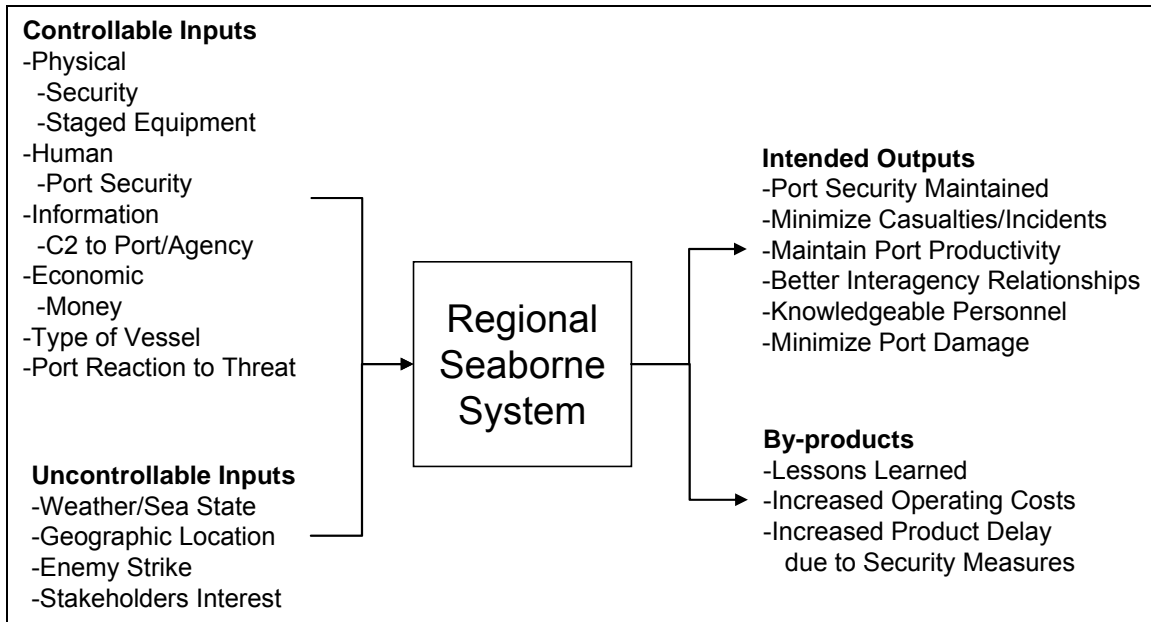


Figure 47. RSTG Input-Output Model

d. Functional Analysis

To effectively mitigate and neutralize the threats posed to port security from the local waters, the functional flow of the port security system is envisioned as:

The sensors for detecting small boats are in continuous operation and scanning for appearance and movements of small boats in the local waterways. Upon detection, the locations of the small boats are tracked. Profiling is performed continuously assessing if the small boats are not following safe routes and/or breaching proximity areas to sensitive installations such as oil and chemical installations, and cruise and ferry terminals. Like in Singapore, small boats could possibly be outfitted with HARTS, and the port would be monitoring for alert signals relayed through HARTS, and if alerted, will notify the port security forces (such as RSN or PCG) to deny, delay, detain or expel the threat. Further efforts will be utilized to classify the small boat, through visual identification to assess whether the boat may be carrying WMDs or conventional weapons. If the probability of such an occurrence is high, countermeasures are put on standby, ready to be activated to neutralize the threat as shown in Figure 48.

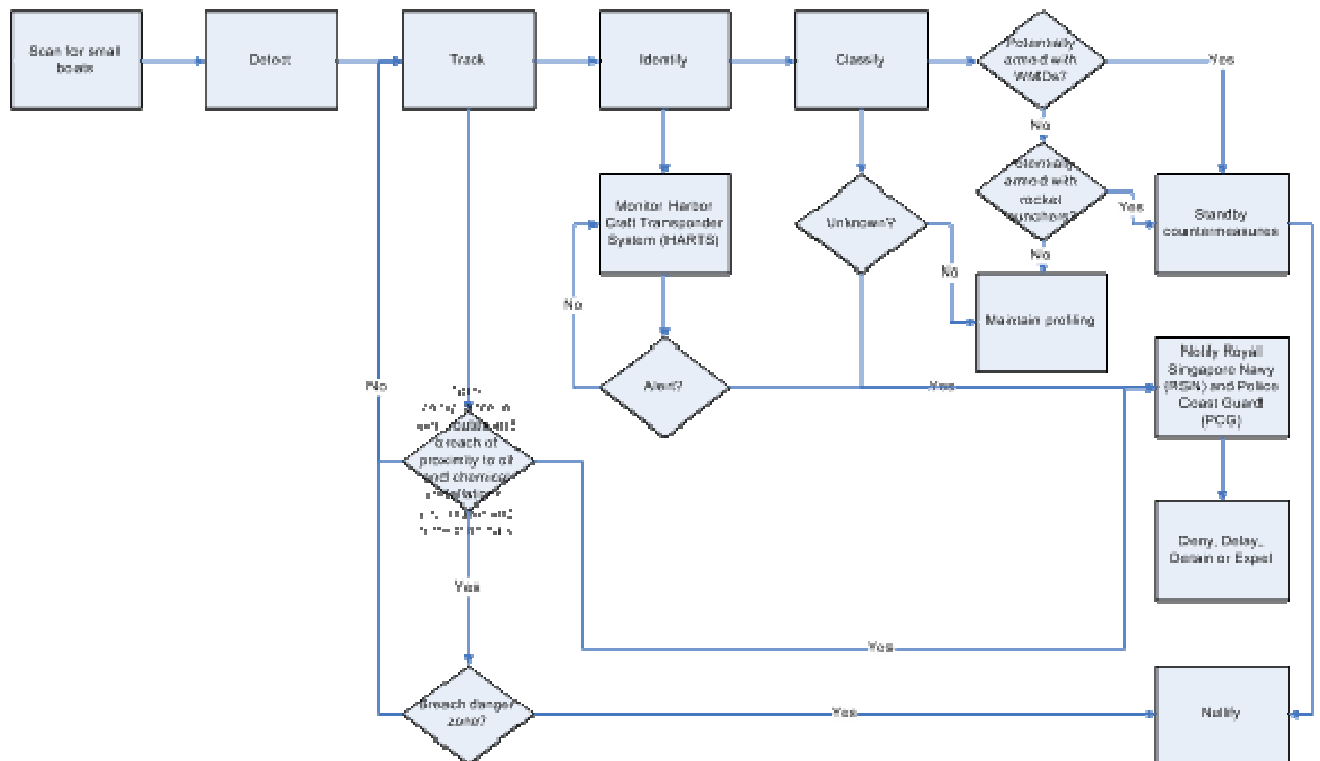


Figure 48. RSTG Small Boat Threat Functional Flow Diagram

The sensors for detecting large vessels would be in continuous operation and scan for appearance and movements of such in the regional waterways. Upon detection, the locations of the vessels are tracked. Profiling is performed to continuously assess if the vessels are not following safe routes and/or breaching proximity areas to the previously mentioned sensitive installations. The vessels should be outfitted with SASS, and the port would be monitoring for alert signals sent via SASS, and if alerted, will notify the previously mentioned port security forces. The vessel would be identified through AIS and PANS, and anchor at a designated anchorage to be subjected to ship self-security verification and face-to-face checks by security and/or immigration officers. If the check and profile of ship or crew and passengers indicates a high probability of WMD, countermeasures are put on standby, ready to be activated to neutralize the threat as shown in Figure 49.

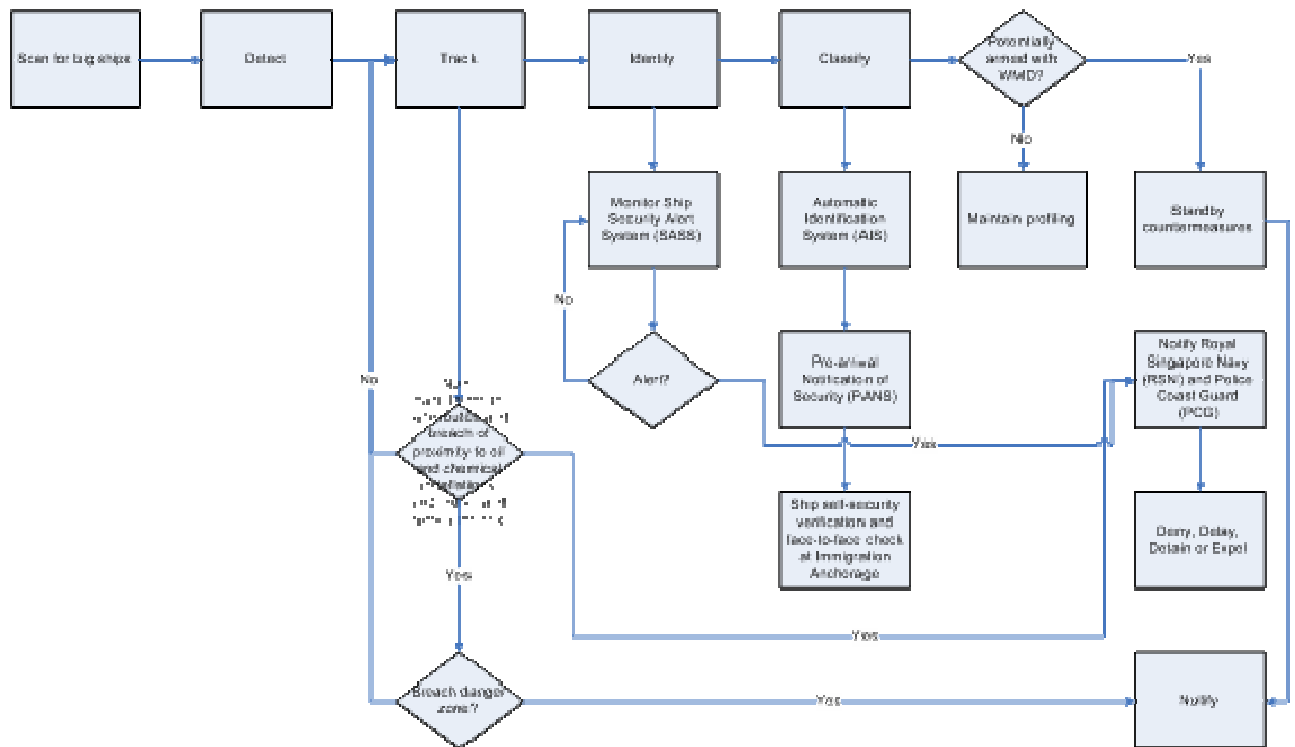


Figure 49. RSTG Large Ship Threat Functional Flow Diagram

Likewise, the sensors for detecting divers or swimmers are in continuous operation 24x7 and scanning for evidence of divers and swimmers in the local port vicinity. Upon detection, the locations of the divers/swimmers are tracked. The port security forces would be activated to neutralize the threat. If identification and classification of divers or swimmers indicates high probability of WMDs or explosives, countermeasures are put on standby, ready to be activated to neutralize the threat as shown in Figure 50.

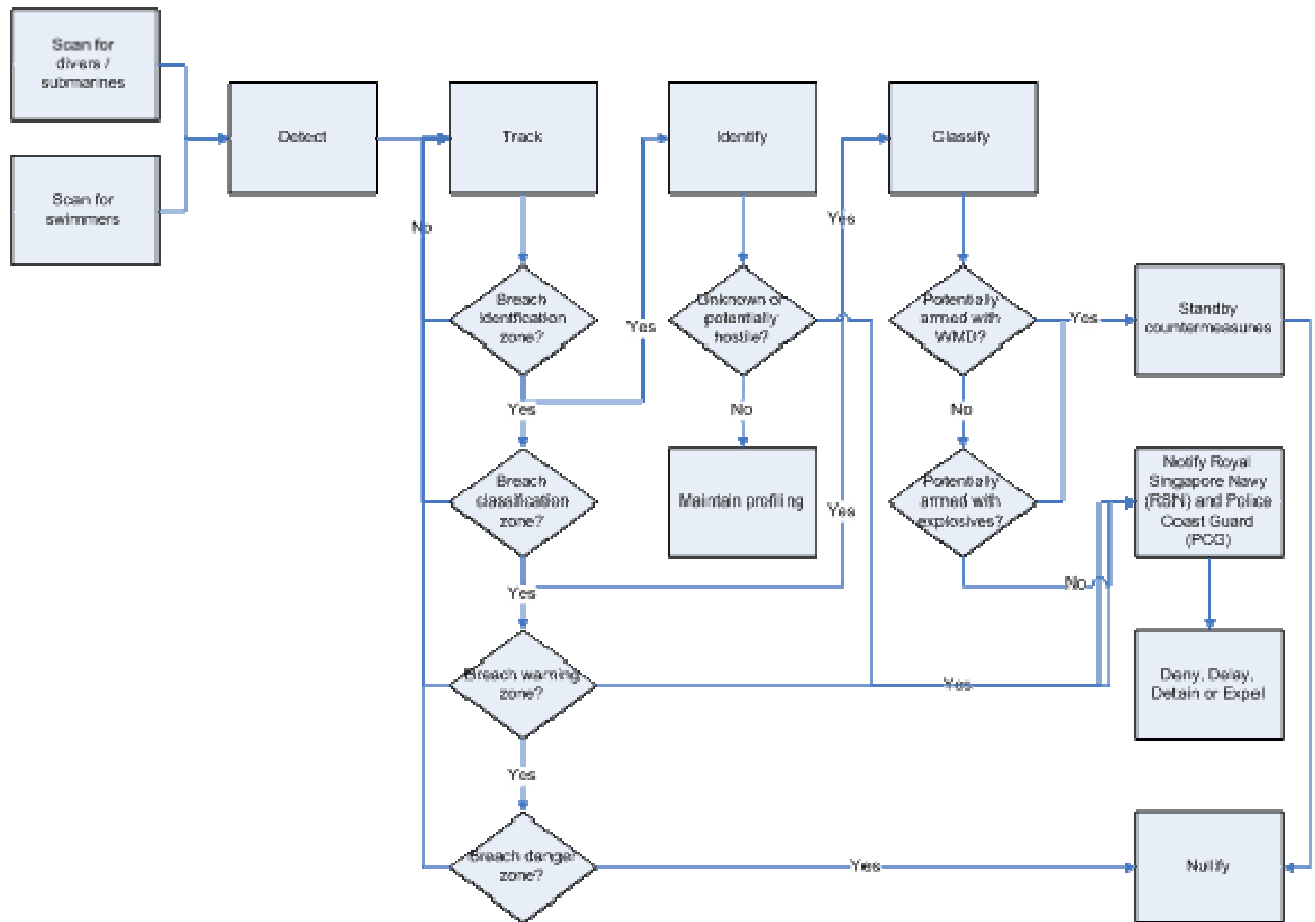


Figure 50. RSTG Sea Inserts Threats Functional Flow Diagram

2. Objectives Hierarchy

In Figure 51, the need is to supply a protective element for force protection and port security. With pier waterside standoff, there is a clear and present threat to the operability and functionality of the ports to supply force protection to moored vessels. When ships are discussed, it pertains to the commercial and military vessels. When ships are moored to a container terminal, it is the responsibility of the terminal as well as the ship to protect itself. Detecting is the function of finding a threat which is in the action of committing a terrorist act. Within detecting, scanning is the ability to analyze the area being monitored to look for a type of particular threat criteria that poses a threat to the security of the port or moored ships. Classifying is the next sub-function of detect. Classify involves assigning a classification to a threat that was detected because it met a certain threat profile. Tracking occurs when the system in place monitors the line of

motion of the threat. Tracking provides the means to predict the path of the vessel and forecast the target in which the terrorist wishes to attack. Once tracking occurs, the reactive element of engagement takes place. Engagement is the element which shows intent of the threat. There are two aspects of engaging: deny and deter. Deny is to use either lethal or non-lethal means to prevent the penetration of the port and inflict damage to the port or ships. Depending on the intent of the threat, the level of force will be used would vary. Besides deny, deter is to discourage or restrain the possible threat to the port from occurring. By the use of non-lethal force such as loud speakers or high intensity lights, the possible threat vessel is alerted of the situation and alters course and moves out of the area. This objective hierarchy is needed to provide a high level of force protection and allowing a higher level of port security.

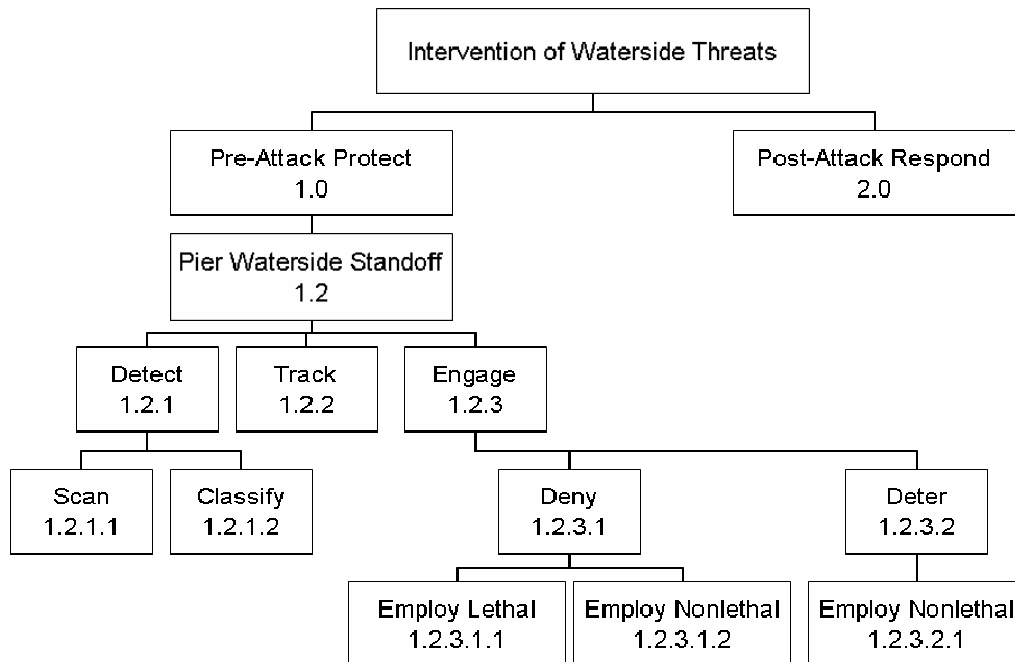


Figure 51. RSTG Objectives Hierarchy

In the analysis of the two broad aspects of the project scope (force protection and port security), relevant MOPs and MOEs have been identified in Table 13. The list of MOEs and MOPS will be classified and associated to its respective objective item from the objective hierarchy illustrated above.

MOEs/MOEs			Objective Item
MOE :	Target Search		Scan – 2.1.1
	MOP:	Search Rate (This is the frequency at which target search is conducted.)	
MOE:	Target Detection		Scan – 2.1.1
	MOP:	Average Range of Detection	
	MOP:	Average Target Detection Time	
	MOP:	Proportion of Detection	
	MOP:	Proportion of infiltrations	
MOE:	Target Classification		Classify – 2.1.2
	MOP:	Proportion of Correct Classification	
	MOP:	Average Range of Classification	
	MOP:	Average Elapsed Time from Target Detection to Classification	
	MOP:	Average Time from Identification to Classification	
MOE:	Target Recognition		Track – 2.2
	MOP:	Average Time from Detection to Recognition	
	MOP:	Average Range of Recognition	
	MOP:	Average Time from Target Recognition to Identification	
	MOP:	Average Range of Identification	
	MOP:	Proportion of Incorrect Identification	
MOE:	Target Tracking		Track – 2.2
	MOP:	Average Distance between Uncorrelated Tracks	
	MOP:	Average Tracking Error (error between sensor tracked location and the target's actual location)	
	MOP:	Proportion of Tracking Time lost	
	MOP:	False Track Rate	
MOE:	Engagement		Employ Lethal 2.3.1.1
	MOP:	Average Range of Engagement	
	MOP:	Proportion of No-Engagement	
MOE:	Timeliness		Employ Lethal 2.3.1.1
	MOP:	Engagement Rate	
	MOP:	Proportion of Encounters where Threats Fired/Attacked First	
MOE:	Effect		Employ Lethal 2.3.1.1
	MOP:	Proportion of Target Engagements vs Acquisitions	
MOE:	Target Handoff		Employ Non-lethal – 2.3.1.2, 2.3.2.1
	MOP:	Proportion of Completed/Successful handoff	
	MOP:	Average of Number of Handoff	

Table 13. Evaluation Metrics for RSTG Objectives

B. DESIGN AND ANALYSIS

1. Alternatives Generation

The alternatives were generated based on the respective detection, tracking, and engagement requirements. Based on the list of available platforms that could be used for the security of the port as well as its surrounding waters, a suite of sensors, weapons and

other forms of detection, tracking and engagement options were proposed. These serve as the building blocks for the proposed systems.

Table 14 summarizes the platforms, sensors, and engagement options which could be used in maintaining security of the surrounding water.

Platforms	DETECT	TRACK	ENGAGE	
			Non-Lethal	Lethal
shore	passive sensor array	AIS	Flares	CIWS
ship		IFF	EMP	missiles
unmanned vessel (ASV)		HARTS	high power lights	
buoys	<i>Surface:</i>	RADAR	Barriers (fences)	
pole	Communication	human	Signs	
unmanned a/c (UAV)	IR	marine mammals	water hoses	
autonomous underwater vehicle (AUV)	Video/Visual	IR	LRAD	
satellite	Laser	OTH	Gas	
	HUMINT		Laser /Dazzlers	
manned a/c	Seismic		Microwave	
	magnetic			
	OTH			
	<i>Subsurface</i>			
	acoustic (active/passive)			
	Seismic			
	magnetic			
	marine mammals			

Table 14. RSTG Possible Platforms, Sensors, and Engagement Options

For example, the port could use wide-area surveillance radar located on the shore to detect potential incoming threats. When a suspicious track has been detected and established, a tracking radar from the shore or a UAV equipped with a camera could provide the necessary tracking capability. This would enable the security agency to monitor its movement before deciding on which course of action to take (lethal or non-lethal engagements) to repel the perceived threat.

The following provides a brief summary on each of the individual platforms, sensors, and engagement options described above:

PLATFORMS

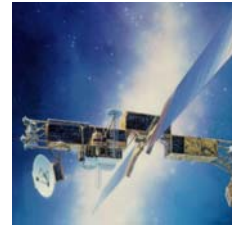
- ***Shore.*** Enhance existing port facilities and technology to increase the ability to detect, track and engage the identified threats.
- ***Patrol Craft.*** Conduct regular patrols in territorial waters, providing frontline support to maritime security in the realm of detection, deterrence and engagement of threats.
- ***Autonomous Unmanned Vessel (AUV).*** Use of advanced technologies to supplement detection of threats. Sensors and cameras could be mounted on the AUV for detection capabilities to scan the terrestrial waterways for threats.
- ***Unmanned Surface Vehicle (USV).*** Are remotely operated vehicles on the water surface or subsurface, the USV could be employed to engage suspicious intruders instead of direct human intervention, especially at distances which may compromise the safety of security personnel.
- ***Buoys.*** Static floating devices which could be mounted with surface and subsurface sensors, video surveillance, or communication relay links to increase broadcast coverage distance.



- **Unmanned Aerial Vehicle (UAV).** A mounted payload as IR/TI camera, sensors or weapons provides day/night aerial surveillance of terrestrial waters up to the horizon for NLOS detection and engagement.



- **Satellite.** An information gathering satellite could be used to track vessel traffic movement towards terrestrial waters from their source port. The ability to detect irregularities in vessel planned voyage allows advance warning to port to take early precautionary measures.



- **Poles.** Are platforms where the sensors could be mounted? A pole could offer increased height for the sensors to achieve a larger coverage range.



DETECT

- **Passive Sensor Array.** Are arrays of hydrophones placed along coastal water, the acoustic sensors detect incoming surface vessels or swimmer intrusion through propeller beat, cavitation, propulsion machinery noises, and hull vibrations. These arrays are able to incorporate the ability to reject underwater sounds not produced by valid targets such as marine life and require long length of cable to cover the harbor distance. **Daily harbor traffic increases the difficulty for the array to distinguish between threats and false alarms, when both are 'intruding' into the waters.** Passive sensor arrays could be used for perimeter-sensing of key installations to detect non-authorized vessels in nearby waters.



- **Communications.** Use of on-board vessel communications equipment to track whereabouts of ships and distance from harbor. Communications equipment type may vary from vessel to vessel. This is a passive system as the ship may not respond to interrogation or when operating at different frequencies.



- **Video/Visual.** Use of video cameras to transmit a signal to a specific, limited set of monitors. Closed-circuit television (CCTV) could be used for perimeter surveillance. CCTV systems may operate continuously or only as required to monitor a particular event.



- **Infra-red Sensor.** Provides night vision capability by near infra-red illumination to detect intruders. IR sensors use the intruder's black-body radiation as a function of temperature for detection. The higher the object's temperature, the more infrared radiation it emits. Performance is affected by humidity, atmospheric interference (rain, snow and etc.), ambient light and distance. IR sensors could be integrated to enhance the CCTV camera system in perimeter surveillance.



- **Thermal Imaging (Laser).** Thermal imaging lasers detect infrared radiation from objects at the scene and create an electronic image. Thermal imagers are entirely ambient light-level independent as they do not rely on reflected ambient light. In addition, they are able to penetrate obscurants such as smoke, fog and haze. Thermal imaging lasers are able to detect people and platforms at great distances, perform high speed infrared imaging, and multi-spectral infrared imaging.



- **Human Intelligent (HUMINT).** HUMINT requires intelligence information gathering and analyzing information on possible terrorist activities. HUMINT provides advance warning against possible threats and heightens securing measures.



- ***Seismic Sensor.*** Seismic sensors provide excellent performance in detecting low-noise vibration. If these seismic inputs meet the pre-programmed requirements for intruder detection, an alarm could be sounded to warn operators.



- ***Magnetic Sensor.*** A magnetic sensor varies an output voltage in response to changes in magnetic field intensity. They are used in mine detection operation with UUVs.



- ***Acoustic (Passive/Active) Sensor.*** A microphone, seismometer, and hydrophone are examples of acoustic sensors. A hydrophone is a sound-to-electricity transducer for use in water or other liquids, analogous to an ear for listening to underwater sounds for detection purposes.



- ***Marine Mammals.*** The Biosonar Program has constructed the world's first biomimetic (think bio mimic) sonar to try to emulate dolphin sonar and incorporate search strategies that are specifically effective in the noisy near-shore environment. This is to emulate a dolphin's highly sophisticated, natural sonar (biosonar) that allows them to detect objects in the most complex of acoustic environments.

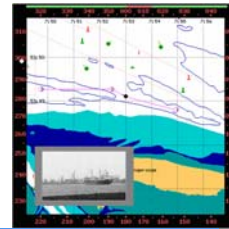


TRACK

- ***Automatic Identification System (AIS).*** AIS is a collision avoidance tool, mandated by IMO SOLAS V, to improve the situational awareness of the bridge crew while facilitating communication between vessels. AIS identifies radar contacts by Maritime Mobile Service Identity (MMSI) and access to accurate positional information for AIS-equipped vessels. Use for text messaging between vessels and/or shore station facilitating communication of maneuvering intentions or safety alert.
- ***IFF.*** Identification Friend or Foe (IFF) system is used as a means of positively identifying friendly forces from enemy. This system relies on equipment aboard a ship known as a 'transponder'. The transponder is a radio receiver and transmitter operating on a radar frequency. The target ship's transponder replies to signals from an interrogator (usually, but not necessarily, a ground station co-located with a primary radar) by transmitting a coded reply signal containing the requested information.
- ***Harbor Craft Transponder System (HARTS).*** Harbor craft less than 300GT and not engaged on international voyages, do not come under the SOLAS Regulations and hence not required to carry the Automatic Identification System (AIS) transponders. Singapore's Maritime Port Authority and the security agencies, developed a vessel tracking system known as HARTS as an added defense against potential threats of attacks by small craft.



- ***RADAR.*** Radar is an electromagnetic system for detecting and locating of reflecting objects such as aircraft, ships, spacecraft, vehicles, people, and the natural environment. It operates by radiating energy into space and detecting the echo signal reflected from an object, or target. It can operate in darkness, haze, fog, rain, and snow. Its ability to measure distance with high accuracy and in all weather is one of its most important attributes.



- ***Human.*** Humans could be deployed at observation locations to observe, track and report suspicious vessels or unauthorized entry.



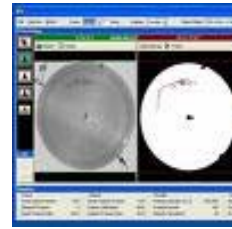
- ***Human Intelligent (HUMINT).*** HUMINT requires intelligence information gathering and analyzing information on possible terrorist activities. HUMINT provides advance warning against possible threats and heighten securing measures accordingly.



- ***Marine Mammals.*** Marine mammals are trained in various roles, which include protecting ports and Navy assets from swimmer attacks, locating and assisting in the recovery of exercise and training targets, as well as locating mines.



- ***Electro-Optics.*** The optical system triangulates the position of the marker using multiple overlapping cameras. It can track multiple targets with its various cameras and other video sources.



ENGAGE: LETHAL

- ***Close-in Weapon (CIW).*** CIW are weapon that are mounted either on shore/ship or both for detecting and destroying incoming threat vessels at short range (500 to 12000 yards).
- ***Missiles.*** Target tracking rockets are able to deliver destructive force (usually in the form of an explosive warhead) upon a target. Besides explosives, other possible types of destructive missile payloads are various forms of chemical or biological agents, nuclear warheads, or simple kinetic energy (where the missile destroys the target by the force of striking it at high speed).



ENGAGE: NON-LETHAL

- ***Flares.*** A type of pyrotechnic that produces a brilliant light or intense heat without an explosion. It is a non-lethal weapon intended to cause temporary blindness or disorientation
- ***High Powered Lights.*** A high powered light source that produces a brilliant light or beam with high visual intensity is a non-lethal weapon intended to cause temporary blindness or disorientation



- **Barriers (fences).** Water barrier could be used to delineate restricted areas while providing both a visual and security barrier in the water.



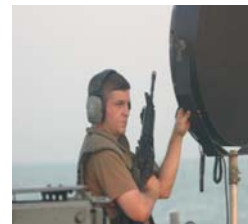
- **Signs.** Signs could be deployed in strategic locations to warn and deter potential intruders or vessels. The signs can be mounted on buoys or floating platforms.



- **Water Hoses (Jet).** Water Jets, which takes water in, accelerates it, and discharges it at high velocity, are used to deter potential intruders from land and sea. It is effectively used in disseminating riots and violent protestors.



- **LRAD.** Long range acoustic device (LRAD) is a crowd-control and combatant-deterrent sonic weapon. The device is used to warn incoming vessels approaching without permission. It is capable of permanently damaging hearing, and 50 times the normal human threshold of pain (120 – 140 dB). The design range extends 300 to 500 meters. At 300 meters, the warning tone is 105 dB. The warning tone is a high-pitched shrill tone similar to that of a smoke detector, only louder.



- **Laser Dazzlers.** Laser dazzlers are a type of a directed-energy weapon that employs intense visible light. It is a non-lethal weapon intended to cause temporary blindness or disorientation



- **Gas.** Tears gas could be used to disorientate intruders and unauthorized entry. Tear gas grenades could be deployed to immobilize the unauthorized vessel in the vicinity of the port.



- **Microwave.** A microwave includes a strong millimeter-wave transmitter used for crowd control or a threat by directing electromagnetic radiation toward the subjects. The waves excite water molecules in the skin causing an intensely painful burning sensation.
- **EMP.** This directional weapon is designed to disable electronics on a small scale. This would be used for disabling a terrorist speedboat or preventing the threat from escaping.



The following matrix of alternatives was proposed.

Shore

This alternative involves detection, tracking, and engagement capabilities, which reside only in the port itself, with no additional ‘forward capabilities’ in the waters itself. This is the current architecture for the Port of Oakland and it is very limited. With shore the Port of Oakland can mainly support detection and some tracking depending on the sophistication and money the facility spends to provide security in support of 33 CFR Part 103 and 105.

Ship/Patrol Craft

This alternative involves detection, tracking and engagement capabilities which reside only in the port itself, as well as with ‘forward capabilities’, such as patrol vessels from the Coast Guard that can perform interdiction in the surrounding waters. This is the current architecture for the Port of Singapore where they use both Navy and Coast Guard

assets to provide a layer defense. The Port of Oakland as well has this capability but at a limited level compared to the Port of Singapore.

Unmanned Surface Vessel (USV)

This alternative involves the use of USVs for detection, tracking and engagement. Although this is currently not in use by either ports, the Singapore Navy is currently exploring the use of USVs for such purposes.

Buoys

This alternative involves to the use of buoys to work as a passive or active sensor array for early detection.

A feasibility study was performed on the various platforms. The process of achieving these alternatives is discussed later in the design and analysis phase for the RSTG. Table 15 summarizes the alternatives considered for the RSTG.

ALTERNATIVES:				
A: SHORE	B. SHIP/PC	C. A/C	D. USV	E. BUOYS
<i>detect</i>	<i>detect</i>	<i>detect</i>	<i>detect</i>	<i>detect</i>
IR Video humint magnetic OTH	IR Video humint	IR Video humint	IR Video	passive sensor array
<i>track</i>	<i>track</i>	<i>track</i>	<i>track</i>	<i>track</i>
AIS RADAR human IR Video	AIS RADAR human IR Video	RADAR human IR Video	IR Video	video
<i>Engage</i>	<i>Engage</i>	<i>Engage</i>	<i>Engage</i>	<i>Engage</i>
Lethal CIWS Non-Lethal LRAD EMP Dazzler Flares lights fence	Lethal CIWS Non-Lethal LRAD EMP Dazzler Flares lights hoses	Lethal CIWS Non-Lethal Flares lights	Lethal CIWS Non-Lethal Flares Lights Dazzler	Lethal Non-Lethal signs

Table 15. RSTG Summary of Alternatives

Based on the derived alternatives in Table 15, the following broad architectures are proposed in Table 16 for the Ports of Oakland and Singapore. Further the use of sensor configuration with the alternatives are then looked at and examined later in the modeling portion of the project.

	Port of Oakland	Port of Singapore
Current Architecture	Shore+Ship+ Manned Aircraft	Shore + Ship + Manned Aircraft
Alternative # 1	Shore + Ship + USV + Manned Aircraft	
Alternative # 2	Shore + Ship + USV + Buoys + Manned Aircraft	

Table 16. RSTG Proposed Port Security Architecture

For the Port of Singapore, besides the current shore-based systems, the respective security agencies are currently operating the following to ensure the safety of Singapore's territorial waters:

Singapore Navy

- Ships – these refer to a fleet of patrol vessels (PVs) used by the RSN.
- Manned Aircraft – these include the Maritime Patrol Aircraft and helicopters.
- USVs – currently used as sensors for maritime operations. There are plans to extend their use to carry weapons.

Police Coast Guard

- Ships – these refer to the fleet of patrol craft used by the PCG.

For the Port of Oakland, besides the current shore-based systems for large container ships out at sea, within the harbor the respective security measures are solely depend upon the port facility itself. The Sheriff's Department and the USCG are organizations for response when a situation occurs at the Port of Oakland as well as other U.S ports. The Posse Comitatus Act prohibits the U.S Navy from acting in a law enforcement capacity within the United States. The level of security for the facilities is set by the USCG and measures that are implemented are proprietary information for the facility. The individual port facility only needs to meet and report the minimum requirements that the USCG enforces. Assets currently surveying the waterways at an infrequent interval to ensure the safety of the port facilities are:

USCG

- Boats – these refer to a number of RHIB vessels.
- Manned Aircraft – these include helicopters.

Sheriff's Department /Police

- Ships – these refer to a limited amount of RHIB (SAFE) designed for SAR missions and port operations. If used in the mission area of port security the assets are limited.

2. System Design Attributes

The following figures provide a visual aid of the environment in which the Ports of Oakland and Singapore operate. The operating environments for both ports have been discussed earlier and will not be elaborated here. Both are busy ports and are potential high value targets for terrorist attacks. It is therefore imperative to ensure that sufficient measures are effective in ensuring port security. Figure 52 shows the operating environment for the Port of Singapore.



Figure 52. Operating Environment for the Port of Singapore

The Port of Singapore is operated by PSA Singapore Terminals. Key security agencies involved in the protection of the port are as follows:

Maritime and Port Authority of Singapore

The MPA is a Government Statutory Board under the Ministry of Transport that regulates and licenses port and marine services and facilities. It also manages vessel traffic in the port, ensures navigational safety and port/maritime security, and a clean marine environment.

Republic of Singapore Navy

The RSN defends Singapore against sea-borne threats and protects its sea lines of communications that encompass the Singapore Straits and its access routes.

Police Coast Guard

The PCG ensures coastal security and maintains law and order within Singapore Territorial Waters (STW). They enforce the law and maintain order in Singapore Territorial Waters and prevent and detect crime. They also conduct Search and Rescue as well as assist other maritime agencies such as the MPA and the ICA, which handles customs and immigration issues.

The Port of Oakland is operated and leased to nine privately owned companies. Within the United States, the key security agency involved in the protection of the port is the Department of Homeland Security. The primary contributor to the security of the waterways for the Port of Oakland as well as other U.S. ports about the nation is the USCG. Within each privately operated port facility there is a Facility Security Officer (FSO) who is hired by the company to maintain the security guidelines the USCG place upon the port facility. These FSOs work with the Port Security Officer (PSO) to help provide security for the Port of Oakland. Annually or when required by the USCG, the FSO and PSO meet with the USCG which composes the Area Maritime Security Committee (AMSC) and discuss security matters. Figure 53 depicts the operating environment for the Port of Oakland.



Figure 53. Operating Environment for the Port of Oakland

Within the Port of Oakland, key security agencies involved in the protection of the port are as follows:

United States Coast Guard (USCG)

The Eleventh Coast Guard District is located on Coast Guard Island in Alameda, California along the east side of San Francisco Bay. Their mission is “As Guardians of the Gateway to the Pacific, District 11 serves, protects and defends the American Public, maritime transportation system and marine environment, through innovation, operational excellence, partnership and teamwork, to ensure a safe, secure and prosperous America.” Their mission includes: (1) Responsibility for 3.3 million square miles of coastal and offshore waters extending 1000 nautical miles off the coast of California, south to the Columbian and Ecuadorian border in South America. (2) The maintenance of the ports, waterways, and while providing coastal security. Since the Port of Oakland is designated a Tier One port, maritime protection is required for the safety of commerce. The Homeland Security Advisory System (HSAS) corresponds to the Maritime Security (MARSEC) levels and restrictions are tightened or relaxed accordingly.

Local Authorities

These are composed of local police, sheriff, fire departments that have available assets for assistance. This aspect is small compared to the USCG, but it is an available entity. Jurisdiction is a concern when dealing with multiple law enforcement agencies.

Facility Security Officer

The FSO is responsible for maintaining, acquiring, and operating the security measures at the facility. Depending on the port facilities, some companies have invested

in surveillance cameras at specific locations. When these surveillance assets are limited only to the FSO and not the security personnel, the benefit of the information is analyzed to what the FSO deems important. This disconnect between the FSO and security personnel presents an issue that affects the overall status of port security. Security personnel are members of the local unions that provide the last line of defense against unauthorized personnel access to the port at the access points. They are typically armed with a flash light and a communications device. Since the unions fill the port security positions, the possibility of rotating security officers into key security positions exists. This creates a security breach in which the security officers may not be trusted with the full suite of surveillance capabilities the FSO might have at his disposal. This results in the security guard's reduced functionality reducing the overall security of the port facility.

Based on stakeholder inputs, four potential threats have previously been identified and briefly discussed. They are:

- Small boat attack on port
- Big ship attack at port
- Sabotage from sea inserts
- Remotely launched projectiles

To maintain and ensure security, the port must possess the necessary suite of tools which allows the detection and engagement of threats. An open architecture is required to allow further advances to be added to the system. The requirements to detect and engage the identified threats are:

Small Boat Attack on Port

Small boats can attain speeds of 30+ knots and their small size often allows them to go undetected. As such, it is important to have sensors that have the ability to detect small boats with such small radar cross section (RCS) from longer ranges which allows sufficient reaction time to counter this threat.

Big Ship Attack at Port

Big ships seldom travel as fast as small boats. Their large RCS also allows them to be detected and identified from further distances. However, their large size means that

a significantly larger number and more lethal factors are required to stop a rogue ship approaching the port.

Sabotage from Sea Inserts

Sabotage from sea insert is a threat because of its relevance to ports that have islands in the vicinity. This threat results from the infiltration of personnel into the port to sabotage its infrastructure or deny the operations of the port. Detection would be difficult due to the covert nature of such operations.

Remotely Launched Projectiles

The proliferation of many remotely-launched projectiles (RPG) into the hands of terrorists enables these weapons to be used against the port from small boats that are in the harbors, straits, or nearby islands. The expected fallout from such attacks would be more psychological than physical due to the limited amount of damage that can be inflicted by each weapon. Even under such attacks, port operations are not expected to completely cease. Detection would be difficult due to their small signatures, exacerbated by these time-critical targets do not allow much reaction time once they have been fired.

Based on the four identified threats, it was concluded that the scenario of fast approaching small boats filled with explosives to either detonate at a ship pier-side within the port, or to damage the port itself, seems most likely (e.g. the USS COLE bombing in Oct 2000). All of the following sections will focus on this specific threat and its variations.

Therefore a new revised problem statement for the RSTG is to enhance port waterside security for the Port of Oakland prior to terrorist attack while carrying on daily port operations by detecting, tracking, and employing appropriate courses of action.

The ability to quickly detect these threats is the primary factor to countering them. Tracking and engagement are the next steps once detection has occurred. Hence, it is desired that a minimum engagement range of two km be required. Taking into account the speed of 30+ knots at which a small boat can travel, as well as a reaction time of at least five minutes, the minimum detection range of potential targets should be at least 4.5 km. The following Figure 54 summarizes the results.

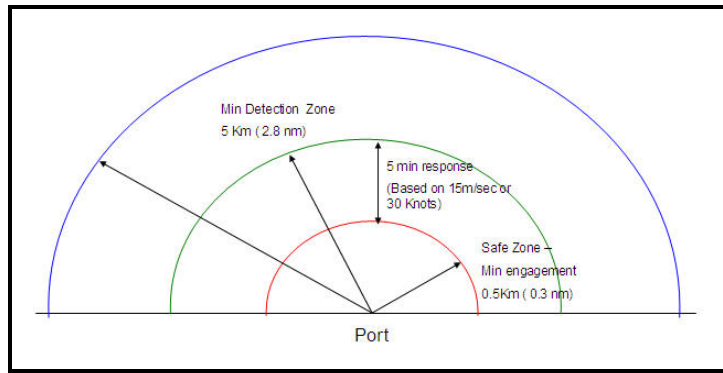


Figure 54. Desired Detection and Engagement Range

However, realistically, it is often impossible to achieve such desired detection and engagement ranges. The high traffic in both ports means that terrorists could potentially hide under the cover of larger ships or general ship traffic to avoid detection and enter the port vicinity. Also, spotting the terrorists before they carry out their plans is extremely difficult.

The proposed implementation of the platforms, sensors, and effectors must be sufficiently robust to handle the various possible scenarios.

3. Feasibility Screening

Conversation among the members in the RSTG yielded a screening process that provided functional and relevant alternatives against a waterborne attack. Feasibility was analyzed by platforms and into the functions of detect, track and engage. This process provided the required tools to examine alternatives in sufficient detail to determine if the minimum requirements of the stakeholders are met. In the feasibility screening, the objective is to eliminate impracticable alternatives. The screening process for the platforms, detecting, tracking, and engaging are:

Platform/Shore

This platform type is very feasible and can be installed inside or outside the port facility. It provides a large area to be covered depending on the height of the sensors. The ability to expand on the sensor package or provide better technological systems is very feasible. Since the time frame is to have it operational by 2012, the deadline is

manageable. There is a chance as more of these shore platforms increase, the sharing of information with other port facilities or even the USCG is more feasible providing better Maritime Domain Awareness for the San Francisco Bay.

Platform/Ship

This platform type is also very feasible and provides the means to position the ship in a location that is ideal for intercepting and engaging a potential threat. Location of the ship is flexible and not fixed to a permanent location like that of a shore platform. Having this unit as an organic asset of the port or an inorganic asset of the USCG provides a functional aspect of maritime protection.

Platform/ASV

An autonomous surface vessels (ASV) provides the same measures as stated above with the ship. Reduced man power is an advantage over the ship. If a threat becomes apparent to the port facility, the threat of personnel casualties is reduced. Port facilities or the USCG can own and operate the asset and the required sensors from a shore location.

Platform/Buoys

With the already installed navigational markers throughout the Port of Oakland, adding passive or active sensors on the buoys is a feasible alternative. These systems can covertly increase situational awareness. Port facilities and the USCG can access the information regardless of the situation or location.

Platform/Poles

This involves placing a sensor on a wood pylon that is anchored to the seafloor. This is infeasible since this would entail adding navigation hazards to the already congested waterway. The ranges and types of systems attached to the pole piling would be limited. Also the functionality of having the sensors on a pylon could be equally or better served on a shore installation.

Platform/UAV

An UAVs is an infeasible option for port security operations. Using the UAV is not practical for two reasons. Government regulations by the Federal Aviation Administration (FAA) restrict the use of UAVs in federal airspace and it is assumed will

not be resolved until after 2012. The launch and recovery of a UAV in the Port of Oakland or at a nearby airport would be restricted.

Platform/AUV

An AUV is an infeasible option for use by port security as a detection and interdiction agent for surface threats. The waterways are not deeper than fifty feet; therefore, the water in which the AUV would operate is limited. Visibility would also be limited due to the increased amount of sediment and sound. The AUV response time to a threat would be reduced compared to the ASV or UAV. Being able to distinguish threat perimeters would also affect the overall efficiency and functionality of the AUV. The disadvantage of having an AUV in the water against waterborne threat is the large expense with little gain which renders this option infeasible.

Platform/Satellite

Satellites, like the UAV, will play a vital role in maintaining the MDA picture in the future. Their role will be essential for coastal and open ocean observation. Their field of view is the largest compared to any of the platforms discussed. Their time on station is a great asset for the MDA picture. In the realm of port security, the benefit of using a satellite for port security operations has its limits. Even with the most sophisticated optics and sensors, the ability to distinguish between a hostile vessel and a pleasure craft will be difficult. Time sensitive information needed from the satellite by the designated agency to take action would be too slow to stop a terrorist in the port. Another reason is in space, the satellites would not be solely used for port security; therefore, the ability to use the satellite for port security would be subject to where the priority of port security falls. Finally, the time on station the satellite can maintain to accomplish the mission. The satellite cannot always remain in a single location and the terrorist threat is not scheduled; the ability to use the satellite for port security is reduced to an expensive device with little gain. Therefore, the use of a satellite is not feasible for port security.

Platform/Manned Aircraft

This platform type is feasible and is able to be positioned in a location that is ideal for intercepting and engaging a potential threat. Location of the manned aircraft is flexible and not confined by a permanent location like that of a shore platform. The field of view gives the pilot or observer a broader perspective of port operations. Having a

manned aircraft maintains human awareness to recognize and act on a situation that might seem suspicious. The presence of manned aircraft provides a functional aspect of maritime protection and is deemed feasible.

Detect/Passive Sensor Array

This device is not feasible for two reasons. It is a passive array which provides only bearing information. Because it provides solely bearing information, the chance of identifying a threat is highly improbable. The shallow waters around the port and throughout the harbor the amount of background noise from container ships to small pleasure craft would render this system to be ineffective.

Detect/RADAR

The use of RADAR is feasible and provides the means to detect and track contacts. By evaluating the vessel attributes, the intent of the vessel can be concluded. By using RADAR, early detection of possible terrorist threats against the port or merchant traffic is available.

Detect/Communications Devices

Communications involves the use of various types of devices to alert the proper authority of a possible threat. Communication devices are feasible tools to help in the detection. They provide a means to coordinate port security activities.

Detect/Infrared (IR)

IR provides a feasible option for detection. IR may be used during night or day. The thermal gradient between the water and ships can be easily detected by IR devices. IR is not affected by the small RCS of an object, but by the thermal heat produced by the object. The ability to recognize small objects remain. Contacts can be detected by IR in high sea states.

Detect/Video-Visual

Video and visual means provide a feasible alternative for detection. Video detection is currently used by port facilities to monitor containers in the yards and observe personnel traffic. The use of video or guards provides awareness of any terrorist intentions. The improvement in the range of optical sensors technology is ever increasing. This option provides real time surveillance of the threat to the proper authorities.

Detect/Laser

This technology is still in the development stage and therefore not feasible and will not be at the maturity required by 2012.

Detect/Human Intelligence (HUMINT)

This is feasible and is currently used. HUMINT is the use of the other agencies besides DHS to gain intelligence that might help prevent a terrorist attack.

Detect/Seismic

This technology will not be feasible by 2012.

Detect/Magnetic

This sensor is not recommended and thus not feasible for this particular situation. With the number of ships and small boats that travel through the waterways, the reliability of the magnetic sensor is reduced and not effective. The use of fiberglass and other composites for small boats decreases the magnetic signature of the vessel. This decreases the effectiveness of the magnetic sensors placed on the bottom of the waterways.

Detect/Acoustic

Acoustic technology is either passive or active. With the noisy environment in which ports are situated, the benefit of this device is limited. An improved ability to filter background noise could possibly make this device feasible.

Detect/Marine Mammals

The use of marine mammals is not a feasible option. It would be hard to establish the boundaries set for the animals. The range in which these animals could enforce would be restricted. With the waterways providing public access to the Port of Oakland, the chance of an attack upon a benign contact is possible; therefore, the use of marine mammals is not feasible.

Track/AIS-HARTS

The use of AIS/HARTS is a feasible alternative for tracking contacts. All large ships operate an AIS system that reports the position, speed and direction of the vessel. AIS is a device that is monitored by any agency requiring the information. HARTS is similar to the AIS system but used for small boats. This system is already in use in

Singapore and is a tool that regulates and monitors shipping and boating traffic. The use of these devices in the Port of Oakland or any port in the United States would be helpful in surmising the threat a contact might present. The use of the HARTS for small pleasure craft and AIS for larger vessels also provides safety awareness that could be recalled when needed. Overall this device would assist in providing key information to evaluate the intent of a contact.

Track/RADAR

The use of RADAR is feasible and provides a means of tracking contacts. By evaluating the vessel's behavior, the intent of the vessel may be concluded.

Track/Human

This is the ability of a human observer to track a contact of interest while at a watch station. The range of tracking is limited compared to RADAR or the AIS systems. The probability of tracking a contact of interest and reporting to the appropriate agency before the contact completes its mission makes this aspect of tracking by a watchmen ineffective. Using humans to track contacts of interest is relatively slow and deemed infeasible.

Track/Marine Mammals

Same as stated in the detection subsection.

Track/IR

Same as stated in the detection subsection.

Track/OTH

Same as stated in the detection subsection.

Track/Video

Same as stated in the detection subsection.

Engage (Non-Lethal)/Flares

Pyrotechnics flares are a feasible option for port security. These flares could be used to shoot across the bow of an incoming vessel to alert and warn the vessel that it is steering into a restricted area. The range of flares is limited based on the method of release. They could be used day or night and are visual signs which are difficult to ignore. Flares have multiple uses to warn incoming vessels, to request for assistance, and to illuminate the night sky for better situational awareness.

Engage (Non-Lethal)/High Powered Lights

The use of high powered lights is feasible. These lights could be directed at a contact to disorient the operator. The range of these lights and its potential to prevent threat access to the target is limited.

Engage (Non-Lethal)/Barriers(Fences)

Barriers are an effective tool to keep a contact out of a controlled area. Using a barrier within the port and in a restricted waterway is not feasible. Barriers present a political issue with recreational vessels wishing to have access to the public navigable waterways. Furthermore, barriers would slow down the arrival and departure of container ships. The use of a barrier as a means of port security is not feasible.

Engage (Non-Lethal)/Electromagnetic Pulse (EMP)

Electromagnetic pulse weapons are still in the development will not be available by 2012.

Engage (Non-Lethal)/Microwave

This directed energy weapon is a technology on the verge of fruition. The military has a working model called the Active Denial System (ADS). The ADS is a large and bulky unit. It uses a microwave beam to heat the skin to an uncomfortable level and if the contact does not move outside the beam, burning of the skin is possible. It is assumed that this technology will not be portable before 2012; therefore, the use of a microwave beam as a weapon against an inbound vessel is not feasible.

Engage (Non-Lethal)/Signs

The least difficult to implement of the alternatives are signs. They are feasible and provide warning to incoming and outgoing vessels transiting the waterways. The signs provide nothing more than a warning. Their range is limited to a person's eye sight. They assume that a person knows how to read English and their intentions are pure. If the signs are in particular locations and if there is someone standing watch on a particular port facility they provide a imaginary zone which could provide the intent of a contact. For these reasons, signs are deemed feasible.

Engage (Non-Lethal)/Water Hoses

When referring to water hoses as a means of port security, it is in reference to the use of 2.5 inch hoses. Water hoses provide an ineffective tool for fast moving vessels. The range of the water spray is limited to the amount of water pressure (150 psi) that is available. Water hoses are good tools for repelling boarders or for riots and not as a non-lethal measure for port security. The only function that water hoses have when dealing with the port facility is to put out a fire, wash a vessel or supply fresh water to a vessel and should not be considered as an option for port security.

Engage (Non-Lethal)/Long Range Acoustic Device (LRAD)

LRAD is a sonic weapon that can permanently damage a persons hearing as the contact moves within close proximity. This directional beam of sonic energy will initially warn the target, but if the contact continues to move closer, the pain threshold goes beyond the tolerable levels and will harm the aggressor. This alternative is feasible.

Engage (Non-Lethal)/Laser-Dazzlers

The use of a Laser-dazzler is feasible. Laser-dazzlers, directed at contacts, warns and disorients the operator. The level of prevention is limited because the threat could effectively continue on its mission. Laser-dazzlers provide the means to provide what the intent of the vessel is and thereby giving the authorities the right to interrogate the vessel and increase force protection measures.

Engage (Non-Lethal)/Gas

The use of gas is not a feasible alternative. To use gas as a non-lethal measure, many variables need to be accounted for in the application. Against a small fast vessel, the usefulness of gas is questionable. The range is ineffective and the chance of success is minute.

Engage (Lethal)/Close in Weapons System (CIWS)

CIWS is the use of small to medium caliber ammunition for the purpose of disabling a vessel or inflict fatal injury to personnel aboard the vessel. Assets that might have CIWS may be aircraft, patrol boats, or armed personnel. One drawback to the CIWS is the potential to inflict collateral damage. Overall, this was deemed a feasible means to prevent a successful terrorist attack.

Engage (Lethal)/Missiles

The use of missiles is not feasible. Missiles permit a small margin of error within a port or in a waterway. There is a chance that the missile might not strike its intended target. There is also the chance that the missile might not have enough time to arm itself due to the short distances it travels. Lastly, the chance of collateral damage to the surrounding area is also very high when using missiles.

C. MODELING AND ANALYSIS

1. Proposed Detection and Tracking Systems for Modeling

The proposed design was based on the RSTG's evaluation of the main threat from the sea: small boats attacks. The principle consideration in the design of the sensors integration scheme follows:

The RSTG assumed the port authority required five minutes of reaction time from the detection of a contact of interest (COI) to the launch of countermeasures in the form of lethal/non-lethal weapons or a patrol ship to investigate the contact. This requirement results in the need to detect all ships and vessels movements within five nautical miles of the port, initially assuming that a high speed boat closed at a speed of 60 knots. Furthermore, there is a need to monitor and track all vessels activities once they enter the five nautical mile radius.

The concept of detection and tracking is based on the following:

- The first line of detection is radar detection which shall be able to detect small ships or vessels with a radar cross section (RCS) of at least one square meter within the five nautical mile range from the port. Upon detection of the targets, the command center shall track, using tracking algorithm or tracker system, the vessel's movement on its Command and Control (C2) system. Any abnormal vessel movements or routes shall trigger the necessary signal or alarm to the authorities for further investigation and action.
- The second line of detection is the close-in detection. This is achieved through the placing of Electro-Optical (EO) and acoustic sensors at the port to monitor ship activity.
- In addition, the RSTG proposed the insertion of networked sensors to enhance the detection of vessels carrying WMD to the port.

a. Sensor Design Considerations

The types of environment, terrain, target size, distance to track, resolution and operation have to be considered in order to design a suitable sensor suite for the detection and tracking function. Figure 55 shows the effective boundary where the selected sensor suite has to adequately perform the functions of detection and tracking.

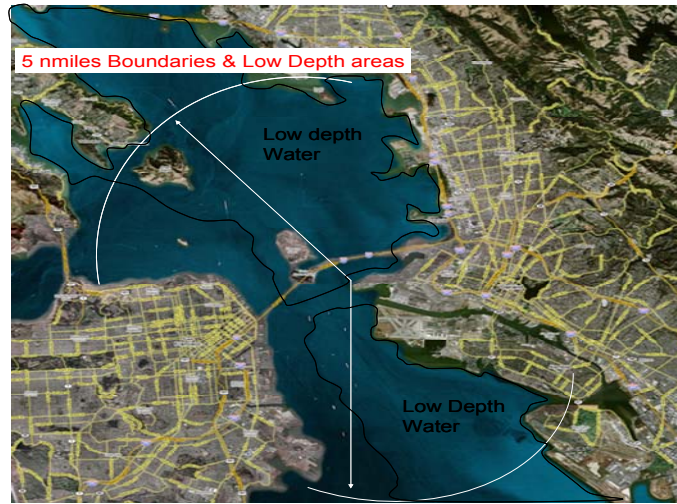


Figure 55. Port of Oakland Detection Boundaries

The sensor has to be able to detect within a five nautical mile coverage area. The next consideration is the size of the target in terms of RCS enabling detection within that distance. The travelling speed of the target(s) would also affect the sensor selection due to the sensor's scan rate. Changes in environment, for example rain, snow, mist and humidity, will affect the sensor's performance and its detection capability. The continuous operating requirement and harsh operational environment presents another challenge in terms of sensors selection.

From the different requirements highlighted, RSTG decided that a sensor suite customised for the Port of Oakland would best serve the intended function. The sensor suite would be a combination of different types of sensors composed of radar, electro-optical sensors (thermal imager and infra-red) and acoustic sensors chosen for their specific function. When these sensors are integrated they would form the sensor suite for Port Of Oakland.

b. Sensor Suite Concept of Operations

Table 17 shows the layered concept of operations for the different sensor types selected for Port of Oakland. The radar would be employed for long range detection but offers a lower resolution. The electro-optical sensors, such as the thermal imager and infra-red sensors, would be installed for close range identification and offering a higher level of resolution. The acoustic sensors placed near key installations offers a relatively rapid detection against close-in threats.

Sensor Type	Operations
Radars	<ul style="list-style-type: none">• All-weather above water surveillance• Long range detection (within 5 nm)• Unified Recognized Surface Situation Picture through sensor fusion
Electro-Optics(Thermal Imager/Infra-Red)	<ul style="list-style-type: none">• All-weather above water surveillance• Upon detection cueing from radars, provide detailed identification of threats at range < 1.5nmi
Acoustics	<ul style="list-style-type: none">• Medium-range medium-frequency active sonar<ul style="list-style-type: none">◦ Cover key installations against surface ships, submarines, small boats, swimmers, divers, AUV• Short-range high-frequency active sonar<ul style="list-style-type: none">◦ Barrier to cover the inner harbor and coastal areas for perimeter detection < 0.5 nm

Table 17. Sensor Suite Concept of Operations

A common operation picture displaying a unified recognized surface situation could be presented to the operators by sensor fusion from the different platforms with the ship's Automatic Identification System (AIS) and interrogation friend-foe (IFF) systems. A system of systems operation can be further achieved by integrating the sensor suite with the port deterrence system for a coherent sensor-shooter operation.

c. Sensor Consideration: Radar

The purpose of radar is to detect all the commercial vessels and small boats within a five nautical mile radius of the Port of Oakland. It is especially useful to

detect fast approaching vessels which could be any of the small boats within the vicinity of Port of Oakland. A small boat could have a RCS as small as one square meter. When this vessel is traveling at a speed of 30 knots, this translates into a reaction time of about one minute per kilometer before reaching its destination at a port. Therefore, the radar must have the sensitivity to detect the small RCS at least five miles removed from the port range to maximize reaction time.

The radar site for sensor installation is to be on the highest ground practicable to improve the detection angle and range to the target. The radar antenna is to be of a wide structure with narrow beam width to detect the small RCS of vessels and to provide adequate noise rejection from atmospheric and maritime clutter. The radar propagated signal waveform has to be at high frequency with frequency diversity to facilitate changing environmental conditions. The radar wave should be of circular polarization to improve performance while raining. Other desirable specifications are detailed in Table 18.

Specifications	Functions
Non-coherent Pulse Modulation	<ul style="list-style-type: none"> • Non-coherent pulses de-correlate sea clutter • Ship echoes stand out stronger • Target velocity derived from range gate integration
Frequency Modulated Continuous Wave (FMCW)	<ul style="list-style-type: none"> • Useful when target has high velocity relative to environment • Good range resolution measurement
Coherent Pulse Doppler	<ul style="list-style-type: none"> • Uses phase or frequency of transmitted and received signals • Allows extraction of both range and velocity from doppler • Discriminate moving targets from weather and other types of background clutter • Relatively immune to simple countermeasures

Table 18. Radar Specifications

Four off-the-shelf radar types were evaluated. Table 19 compares the various radar specifications for detecting a target size of one square meter.

No.	Radar Type	Country	Frequency	Range	Cost	Assessments
1	Scanter Non-coherent	Denmark	X-band	2.4km	\$1mil	<ul style="list-style-type: none"> • Cheap • Good performance for ship detection • Dual frequency version: 19% improvement in detection range • Detect small rubber boat at 2.4 km • Azimuth beamwidth: 0.4°
2	Advanced Coast Surveillance Radar (ACSR)	Israel	X-band	5km	\$1.5mil	<ul style="list-style-type: none"> • Good range resolution • Detailed range resolution not critical • Azimuth beamwidth: 1.5° • Widest among X-band radars
3	Suricate	France	X-band	8km	\$2.5mil	<ul style="list-style-type: none"> • Very narrow beamwidth (0.6°) • Accurate detection • Cue EO/IR sensors with accurate azimuth • Good overall detection capability
4	Giraffe CD	Sweden	C-band	10km	\$3.5mil	<ul style="list-style-type: none"> • Less attenuation than X-band • Expensive • Poorer detection of low-level targets as compared to other X-band radars • Wide azimuth beamwidth (2°) • Good detection capability for airborne platforms

Table 19. Radar Specifications

For the Port of Oakland application, it is desirable to employ radars operating in the X-band frequency thus providing a low lobe angle for good low-level detection of vessels and small boats. Selecting a fully coherent system provides better signal processing in terms of integration. Therefore, two of the Suricate system radars were selected to provide the desired detection coverage and range.

The current existing radar system and coverage area is shown in Figure 56. It can be seen that the area of detection is not as wide compared to the proposed coverage. In order to achieve the desired detection area of five nautical miles, two additional radar sites shown in Figure 57 are proposed for the Suricate system radars installation. After the installation, the two radars will complement the existing radar by improving the detection coverage area to five nautical miles.



Figure 56. Existing Radar Site



Figure 57. Additional Radar Site

Upon detection of threats, the EO sensor systems can be focused for detailed investigation.

d. Sensor Considerations: EO (IR/Thermal Imager)

The purpose of the EO sensors is to focus on detected fast attack crafts and tracking of smaller crafts or even swimmers heading towards the port for detailed investigation. The sensors would interface with the radar system by providing close-in target tracking and the lethal/non-lethal deterrence systems via sensor fusion for an integrated system-of-systems operation. This offers coherency in terms of operations and minimizes the decision making cycle and maximizes the response action. Similarly, for a small craft travelling at 30 knots, the reaction time is increased one minute per $\frac{1}{2}$ nautical mile. Hence, an EO sensor that provides a detection range of three nautical miles provides a response time of six minutes.

The EO sensors offer detection and recognition capability continuously (day/night) and under all-weather conditions when integrated with the radar systems. Table 33 compares five different types of EO and infra-red (IR) sensors specifications detecting a target size of one square meter.

No.	EO/IR Type	Make	Wavelength	Range	Cost	Assessments
1	Brite Star	FLIR	3 - 5 μm	-	\$100k	<ul style="list-style-type: none"> • Thermal Imager • Laser Rangefinder / Illuminator • Designed for aircraft and shipborne platforms • More expensive than Sea Star Safire III
2	Sea Star SAFIRE III	FLIR	3 - 5 μm	-	\$100k	<ul style="list-style-type: none"> • Shipborne Airborne Forward Looking IR Equipment • Thermal Imager, Image Intensifier, Laser Rangefinder / Illuminator, Spotter Scope • Mounted below aircraft or on patrol vessels • Cheaper than Brite Star (better/similar capabilities)
3	ThermoVision Sentry II	FLIR	7.5 - 13 μm	3km	\$82k	<ul style="list-style-type: none"> • Installed at key installation areas for added coverage • Pan/Tilt capability • Better detection range than Sentinel
4	ThermoVision Sentinel	FLIR	7.5 - 13 μm	2.6km	\$36k	<ul style="list-style-type: none"> • Fixed look direction • Good for perimeter surveillance

Table 20. Electro-Optics/Infrared Specifications

For the Port of Oakland sensor deployment, the radar would provide the initial detection of targets while the EO/IR sensors, upon obtaining the cueing information from radars, would focus on the desired target for detailed investigation. The EO/IR sensors have to be integrated with radar as their performance degrades rapidly in high humidity environments because their signal suffers high attenuation. These sensors also have limited fields of view which could be enhanced by software mosaics to enlarge the tracking areas or targets of interest. However, this may result in latency in terms of refreshing real-time situation data due to the additional computer processing.

Figure 58 shows the deployment plan of the EO sensors. The selected sensors are deployed at locations to maximize coverage of interest areas and distance while minimizing the number of sensors to reduce costs.



Figure 58. Electro-Optics Sensors Deployment Plan

Two ThermoVision Sentry II sensor systems are deemed to be necessary to provide coverage for tracking in the three kilometer radius of the port for detailed investigation capability near key installations areas. Five ThermoVision Sentinels are proposed for perimeter surveillance along the port coast against insertion threats from the sea into Port of Oakland. The Sea Star Sapphire III sensor system is proposed to be mounted on patrol aircraft and vessels for enhancement thus achieving day/night tracking and detail investigation capability.

e. Sensor Consideration: Acoustic Sensors

The purpose of the acoustic sensors is to detect fast attack craft near key areas at the Port of Oakland. The acoustics sonar offers high sensitivity detection capability against small craft surface threats such as powerboats and power-jets and has the added advantage of detecting subsurface threats such as divers, submarines, remotely operated vessels (ROV) and autonomous underwater vehicles (AUV). The acoustic sonar is very expensive. They are only proposed to be installed near key areas at Port of Oakland.

Five different types of acoustics sensor were evaluated. Table 21 compares the five different types of acoustics sensor specifications for detecting a target.

No.	Acoustics Sensors	Frequency	Cost	Assessments
1	Passive Hydrophone Receiver Array	10Hz – 5kHz	\$2.5mil	<ul style="list-style-type: none"> • Silent • Much greater range than active sonar • Allows identification of target • Performance affected by ambient noise • Insufficient for detection of underwater vehicles in littoral environment
2	Active Omnidirectional Tactical Sonar	5kHz ($\lambda = 0.3\text{m}$)	\$2mil	<ul style="list-style-type: none"> • Useful in providing exact position of an object • Difficult to identify the target • Any vessel around emitting sonar will detect its emission • Other platforms can detect active sonar at a greater range than detection range of sonar (2-way attenuation & absorption)
3	Active High-Freq Tactical Sonar	50kHz ($\lambda = 0.03\text{m}$)	\$1.5mil	<ul style="list-style-type: none"> • Good resolution • Short detection range
4	Vertical Array Passive Receivers	1Hz – 20kHz	\$500k	<ul style="list-style-type: none"> • Silent • Much greater range than active sonar • Allows identification of target • Performance affected by ambient noise • Insufficient for detection of underwater vehicles in littoral environment

Table 21. Acoustic Sensor Specifications

Figure 59 shows the proposed acoustic sensors deployment near key installations at Port of Oakland. A total of five active omni-directional acoustic sensors and four active tactical high frequency acoustic sensors are required to adequately fulfill these functions. The active omni-directional acoustic sensors are needed for medium range surveillance and confirming suspected contacts that may be threats. The active tactical high frequency acoustic sensors are deployed to address the threat of small craft or swimmers around key assets by providing a sensor barrier covering the inner harbor and coastal areas for perimeter detection less than ½ nautical mile.



Figure 59. Acoustic Sensor Deployment Plan

The acoustic sensors would be deployed at strategic locations overlooking possible threat attack routes. The detection scheme could also be further complemented by positioning the acoustic sensors at transit passageways and channel routes so that any incoming/outgoing vessels may be easily detected. However, this deployment plan can be highly expensive as there are numerous passageways and channels.

The information from the radars and sensors shall be forwarded to an integrated Command and Control system at the command center. This C2 system shall provide the data fusion of the various sensor information to form the common operational picture (COP), which shall be available for all port authorities and interested shareholders. With the COP, it shall enhance the interoperability of the various agencies for all operations.

f. Coastal Patrol Routes

As stated previously, it is desired to monitor all maritime activity within the five nautical mile boundary of the Port of Oakland. This would allow for adequate reaction time and coordination in the event of any intrusion of unwanted craft and personnel to the port. The boundary includes water of low depth, big vessel shipping

channels, beaches and marinas in the immediate vicinity. These regions have activities happening during various times. Figure 60 shows the locations of the vessels routes and marinas that are located in the region. The RSTG has identified a number of marinas within the vicinity where that can be used as launch platforms for potential terrorist activity. These activities could hinder the port operations; thus, it is prudent to provide a close supervision on activities within the five nautical mile radius of the port.



Figure 60. Locations of the Vessel Routes and Marina

In addition to the situation of radars and EO sensors to detect and track shipping activities, the presence of patrol craft in the surrounding waters is prudent to security and safety of the port and ships. Their known presence could provide a strong deterrence to any potential unwelcome activity.

The RSTG proposed the four patrol routes for security forces. These routes were devised to provide the routine, close-in surveillance to the activities on the

coast and ships in the vicinity. The objective of the close-in surveillance is to complement the sensors in detection, especially in the areas of blind spot and small targets intruders.

The patrol craft shall be equipped with Sea Star Safire III EO/IR sensors. These shall provide the operators in the craft the capability to operate in day and night, regardless of visibility and weather conditions.

Two routes, route 1 and route 2, were proposed for the surveillance of the coasts and marinas. These routes were designed in clockwise and counter-clockwise directions. The considerations were to reduce the predictability of the patrol routes and to increase the periodic presence of the patrol craft. These routes would be constantly patrolled with craft launched at regular intervals. Thus at one time, there would be a couple of patrols on the same route. Figure 61 shows the proposed routes for coastal surveillance.

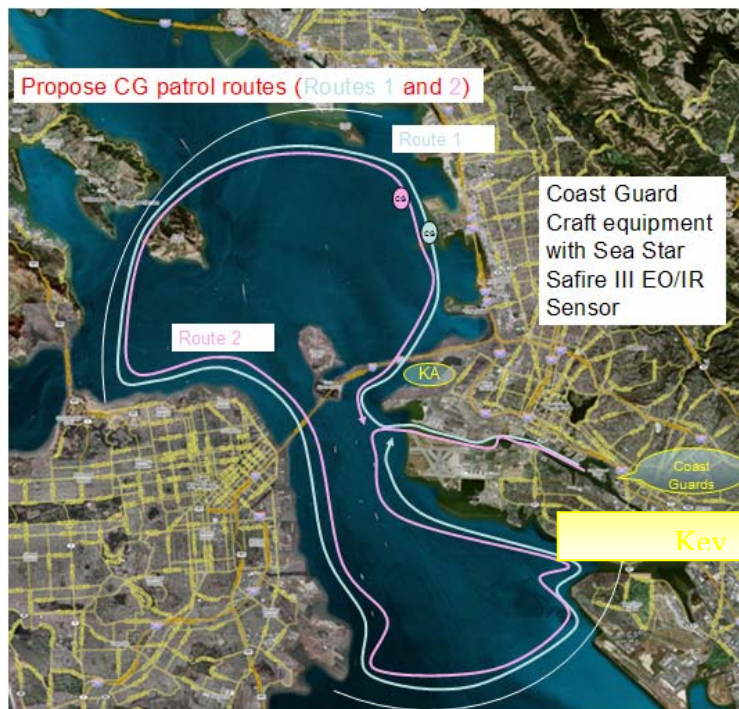


Figure 61. Patrol Routes 1 and 2 (Coastal Patrol)

In addition to the surveillance on the coastal area, the team proposed two inner routes in the sea area for the surveillance of the activities on the shipping routes and anchorage areas. Route 3 and 4 are proposed for patrols in the northern and southern waters of the port. Figure 62 shows the propose routes for the anchorage area. These patrol routes shall provide the surveillance on the activities on the anchorage areas. It allows early identification of abnormal activities or behavior in the ships or vessels.

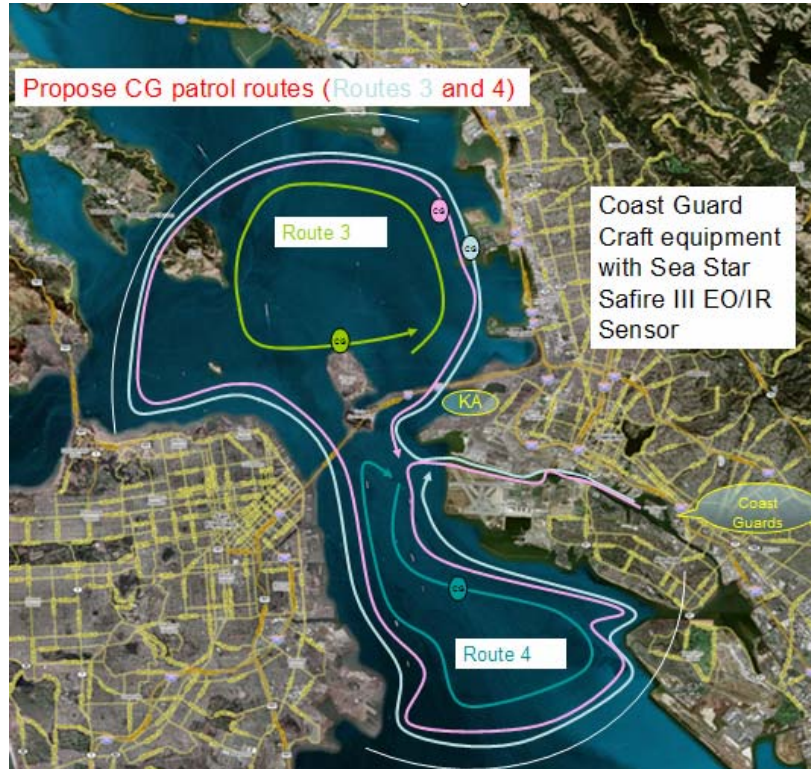


Figure 62. Patrol Routes 3 and 4 (Anchorage Patrol)

The proposed patrol routes created the presence of the security forces in the port vicinity. Through regular contacts with the craft and vessels in the vicinity, the security forces can also complement intelligence gathering, through Human Intelligence (HUMINT), on the collection of abnormal activities and signs of irregular shipment or threats to the port operators or authorities.

g. Possible Routes of Advancement for Small Boat Attacks

Figure 60 showed the location of marinas within the port vicinity where small boat attacks could be launched. In order to evaluate the sensor's detection and tracking capability or hide any early signs of abnormalities of its routes, the intrusive boats were directed to follow the usual vessel routes to move in to the targeted area depicted in Figure 63. Upon closing upon the targeted area, the boats would rapidly detour and move in to strike the port facility.

From the launch platforms to the strike area, the teams devised six possible boat routes which were deemed to have good concealment within the sea routes for vessels and crafts. The initial movement of the contacts of interest was designed to appear to be following the routine shipping routes. These movements are shown in Figures 63 and 64.



Figure 63. Threat Routes: Possible Advancement Routes from Near Bank Marinas

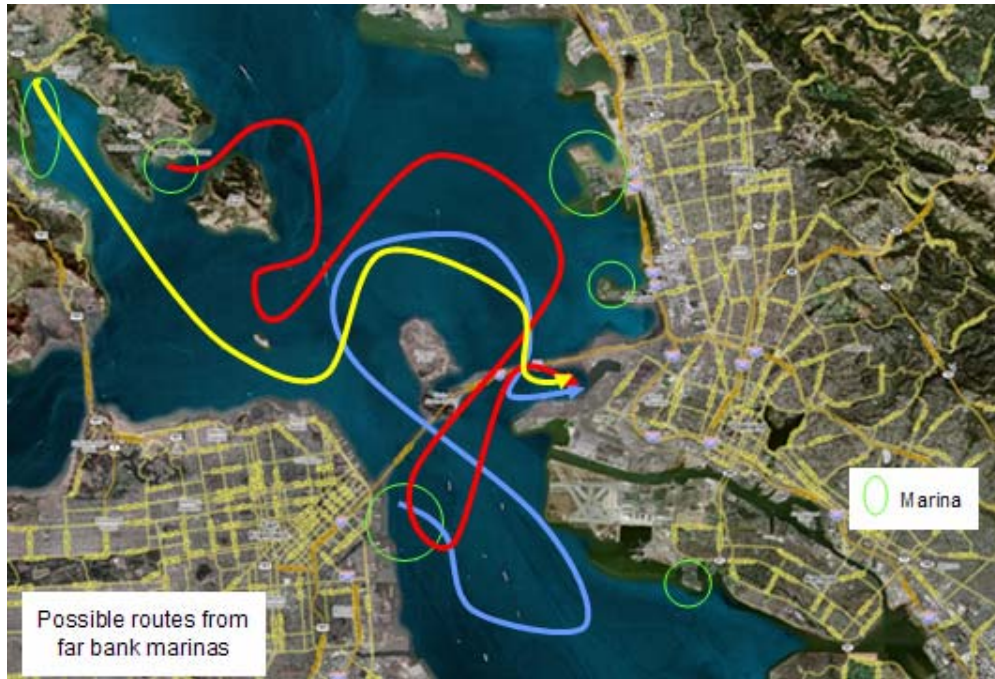


Figure 64. Threat Routes: Possible Advancement Routes from Far Bank Marinas

A simulation program was developed by the RSTG. It aimed to model the projected radar and sensors deployment, security/patrol vessels surveillance routes and the possible threat advancement routes. The programs modeled the proposed solution based on the sensor's specifications on its range, area of coverage, the screening forces on patrol, and the intrusion activities described above. The objectives were to measure the effectiveness of the proposed solutions in their detection capability and the optimal sitting of the sensors for a full sea coverage and detection of small boat activities in the vicinity of the port.

2. Modeling Plan

Faced with the constant increase in complexity of both the components of the system and their multifaceted interrelationships, the RSTG needed a tool to simplify the interactions and provide a visual interface. Modeling is the one tool that helps make the complex situation for the RSTG understandable. For the RSTG, the focus is on the prevent/protect element of force protection and port security. The different alternatives that have been generated for RSTG were prioritized on the probability of specific threats,

identification of key elements of concern for the Port of Oakland, and the resources whose technological capabilities and viability provide security for the port. One way to illustrate the effectiveness of an alternative, or if time and resources permit different alternatives, is to model the problem space and implement the alternatives and execute simulation runs to analyze the results that are collected.

A simulation and modeling tool was selected to execute the design and implementation in the simulation of the alternatives. Simkit, a Discrete Simulation Engine from NPS Modeling, Virtual Environment and Simulation (MOVES) curriculum was selected to carry out the modeling task. Simkit has been used in several Port related analysis projects in the past with positive results. The event-driven paradigm has been popular in MOVES and its modularity is certainly helpful to allow a simulation application to be developed for the RSTG. Agent-based simulation could have been chosen to carry out the development of the simulation for the RSTG; however, most agent-based simulation systems work on the basis of a discrete time paradigm. Unlike the event-driven paradigm, discrete time paradigm advances in unit time steps in carrying out each simulation run. This characteristic has certainly raised some constraints and ambiguity in employing agent-based simulation for the RSTG. One basic constraint would be the need to spend the required number of time units for each simulation run. Collect statistical results based on multiple runs would have been an arduous, if not impossible task. Another ambiguity in using agent-based approach would be the selection of the correct time unit as basis for discrete time advancement. The question of adequacy of a basic time unit has to be defined with respect to the resolution of details that the simulation run is able to capture versus the extent at which physical time would be needed to complete a single scenario run.

In using the discrete event paradigm upon which Simkit is based, the constraints and ambiguity faced with the discrete time paradigm do not surface. This is primarily due to the fact that the advancement of the simulation is purely on the existence of events that exist in time. Simulation run proceed in accordance to the orderly occurrence of events. Carrying out multiple runs to collect statistical results would be much more viable. There

is no need to address the adequacy of the resolution of a unit time interval. Resolution hinges on the complexity of models entirely.

However, there are some agent-based simulation systems that have been around earlier than Simkit. As such, there is a convenient Graphical User Interface (GUI) to facilitate modeling that is currently not available in Simkit. Simulation models developed using Simkit have to start from scratch. Nevertheless, there are several libraries of behaviors that have been helpful.

The analysis of the status quo, identification of the key areas within the port, and the operational approach of the alternatives are key elements that drive the requirements specifications for the modeling and simulation approach.

With respect to the sections that described the alternatives in detail, a flow chart illustrates the flow of an alternative. In this flow chart, for the RSTG, a series of major blocks has been identified. These major blocks for sensory system represent a significant step in the operational procedure that has been formulated in the alternative generation. The major steps are:

- Target Detection
- Threat Classification
- Threat Recognition
- Threat Identification
- Engagement
- Intent Monitoring

Figure 65 represents the flow chart for the RSTG model, which identifies the system procedure in dealing with the small boat threat.

Port Security - Local Waterside - Small Boat Procedure Flow Chart

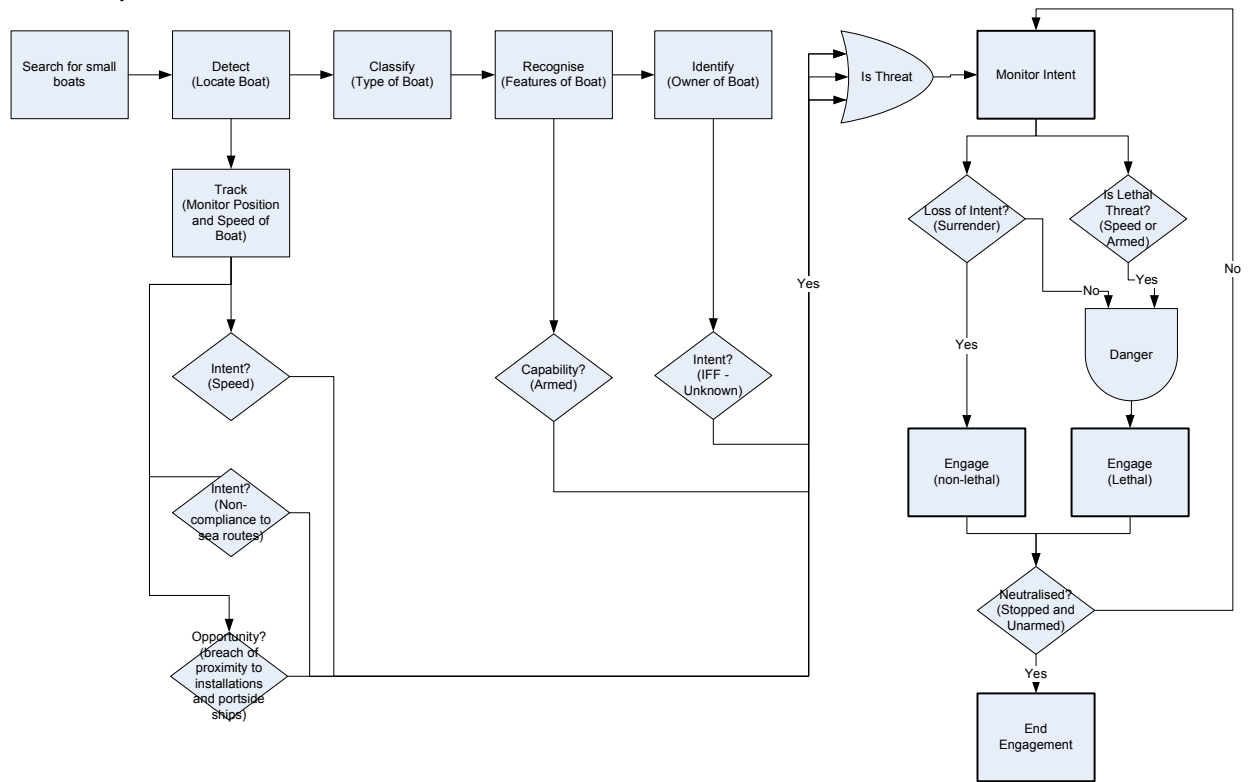


Figure 65. RSTG Model - Small Boat Procedure Flow Chart

The analysis of the alternative has also facilitated the allocation of these major steps linking them into a logical flow. This logical flow depicts how the alternative will be executed in the implementation of the simulation models. The running of the simulation will execute according to the flow analyzed in this flow chart for the alternative.

3. Modeling Explanation

In designing the simulation models, the behaviors for both the threats and sensors had to be created. Different components had to be designed. Each component that was designed had its roles and responsibilities identified with respect to one or more major blocks in the flow chart. The relationship and the communication between components had also been designed to realize the logical flow of procedure that is depicted in the flow chart. In this way, executing the simulation run realizes the execution of the flow chart

logical flow for the scenario that has been created for the alternatives of the RSTG problem space. Figure 66 shows the discrete events considered by the RSTG.

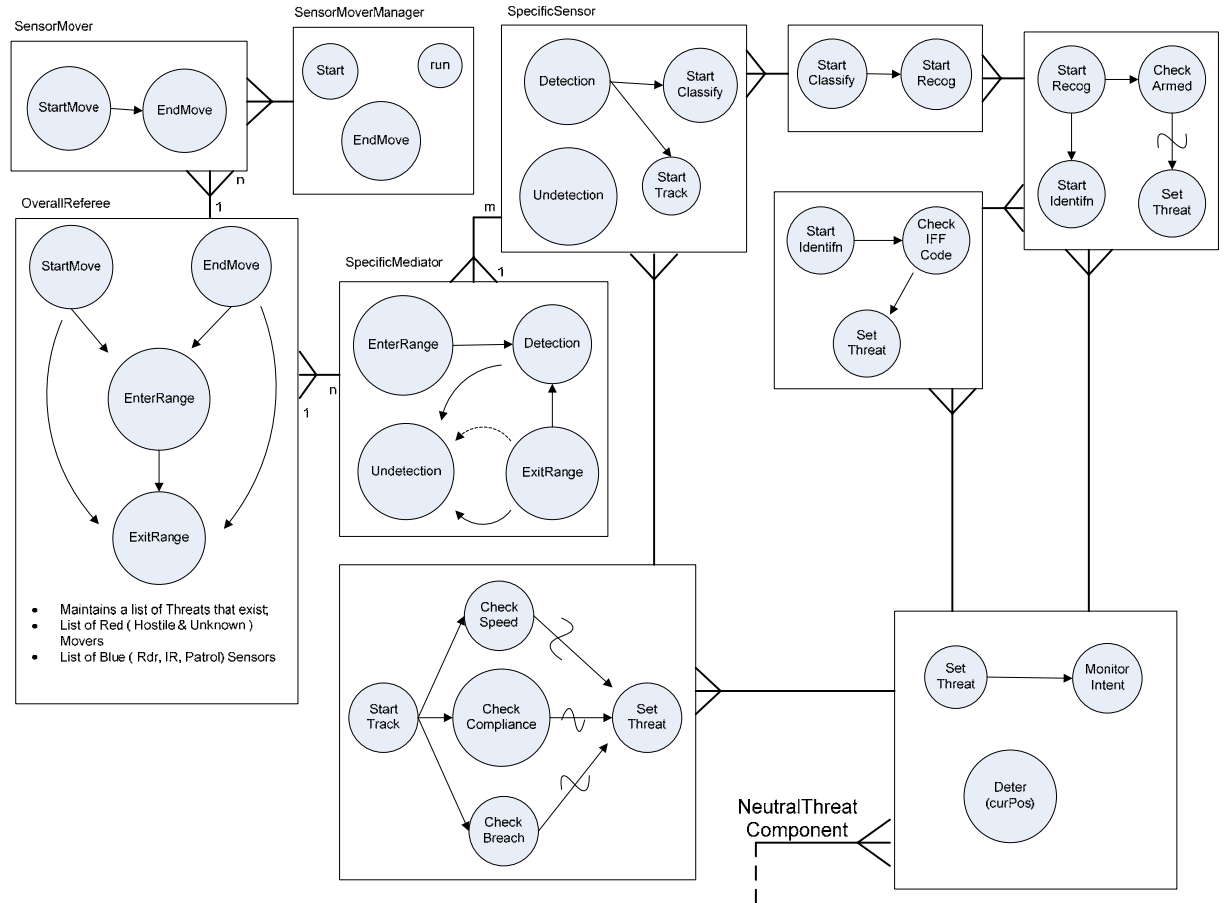


Figure 66. RSTG Discrete Event Components

The components have been designed with the relevant roles and responsibilities that they represent and thus model concrete entities' behavior. There are relationships that link these components together. These communication links implement the relationship between various independent components. These communication links essentially establish the interface to address the independence, extensibility and expansibility of each component in the simulation design.

In the design of the software components, there has been consideration for ease of future expansion and extension on the behavior that is currently implemented. Each

component has been identified with a set of roles and responsibilities. The interface and communication linkages with other related components have been appropriately designed. The current implementation for each component is in fact independent. In the future, when there is a need to change the implementation of one component with a higher precision or fidelity, it could be easily expanded by adding more events without affecting other components. Similarly, when new components need to be created to augment the behavior of existing component, they could easily be linked to existing components without disrupting the other existing components already in place.

The key for ease of carrying out future work using the existing components designed for RSTG would be to fully understand the rationale in the design of each component, its assigned role and responsibility and its existing behavioral fidelity.

The following are some of the simulation components that have been identified. The sensors are the resources that help provide the security of the port while the threats are the behaviors that depict the infiltration of threats to attack the port. The following simulation components are required:

- SensorMover – entity holder that contains the properties of craft, radar and other sensor resource.
- SensorMoverManager – a manager category of object that is responsible in the maneuver of the entity that it is entrusted with.
- Mediator – a category of objects that undertakes the responsibility to facilitate the sensor in the detection of objects of interest
- Classifier – a component that is responsible for carrying out the necessary intelligence of classification of objects
- Identifier – a component that is responsible for carrying out the necessary computation of identification
- RouteDeter – a component that has the role to make decision on making change in the route that the entity will proceed with
- Arrival – a component that is responsible for depicting the existence of threats in the scenario
- CreateThreat – a component whose role is to identify the different types and location where threats will be created in the scenario

Figure 67 shows the user interface for the scenario controller. The user would deselect the visual simulation to box to generate statistics. The number of simulation replications and the number of terrorists can be specified. The array of available sensors can be toggled by selecting and deselecting the appropriate boxes. The positions, routes,

coverage for the sensors, patrols, and threats are described in detail in the following sections.

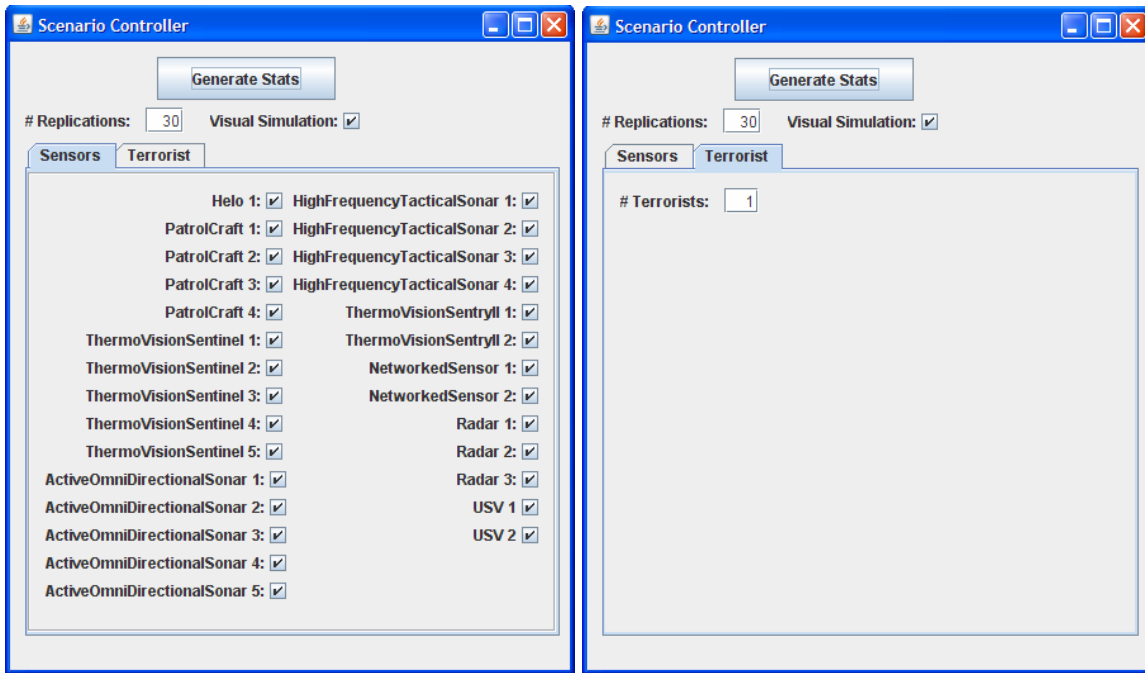


Figure 67. Scenario Controller of Port Security Local Waterside Model

Figure 68 is a screen capture of the RSTG model using Simkit and applied with a “Google Earth” overlay of a section of the San Francisco Bay which contains the Port of Oakland. The user may click on start, pause, step, and stop to run the visual simulation.

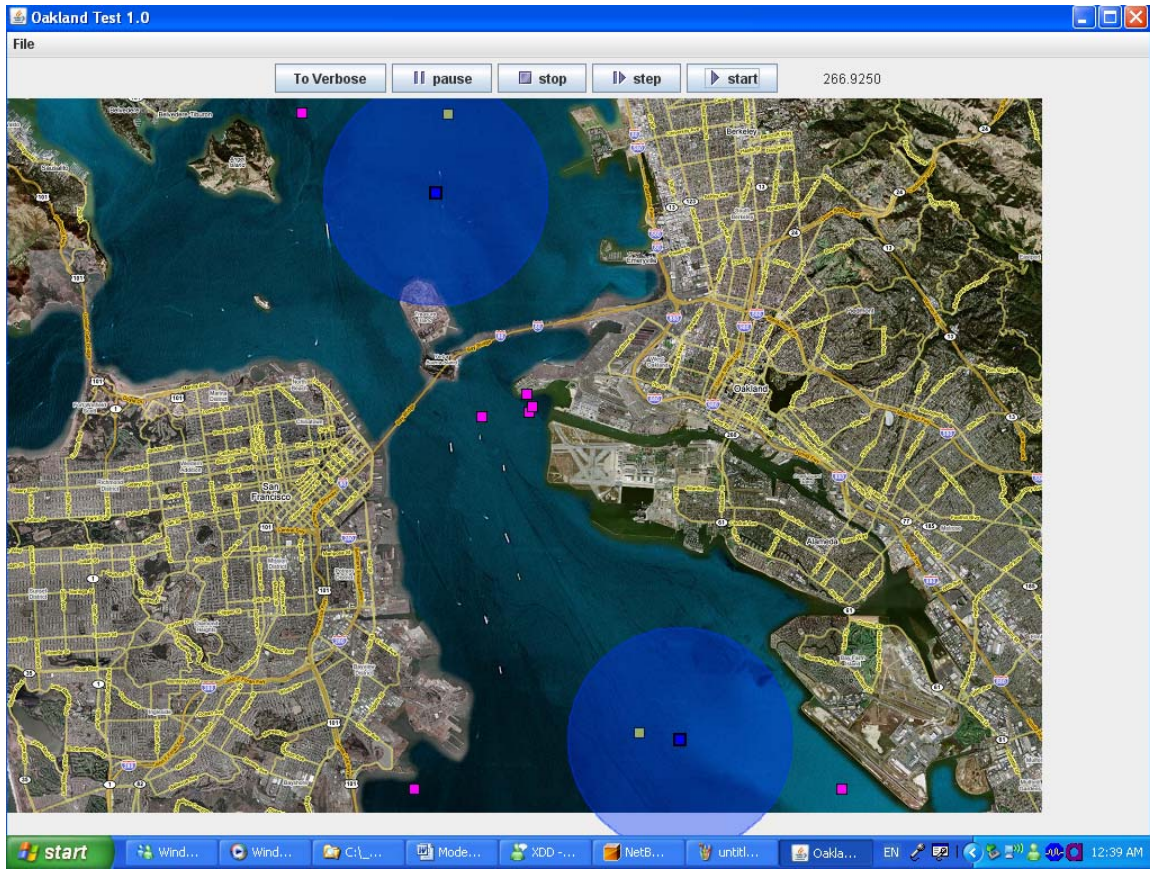


Figure 68. Visual Simulation of Port Security Local Waterside Model

In the application that the RSTG has developed, there are typically seven color schemes used for all entities.

- Blue - depicts the patrol crafts, helicopters, USVs, radar sensors, electro-optic sensors, acoustic sensors, and all entities within the simulation that are considered resources belonging to the agency that is responsible for protecting the port.
- Red – depicts the threats that exist as it would in reality. Contacts that have the intent to infiltrate into the key installation areas through water passage compose the red forces.
- Green – depicts the various pleasure crafts that transit along the waterways of the Port of Oakland. They neither have the ill intent of infiltration nor to attack the port. They are privately owned vessels that ply through the waterway.
- Magenta – depicts all initial contacts, whether threats or pleasure craft or container ships, as unknown. After detection, classification, recognition and final identification, they will eventually update to Red or Green.

- Yellow – depicts a contact within scanner range whose intentions are still unknown.
- Pink – depicts a successful classification of the contact (while in scanner range).
- Orange – depicts a successful identification of the contact (while in scanner range).

The RSTG ran the model more than thirty times for each of the alternatives. This provided an appropriate sample size for a normal distribution for data analysis and provided enough information on which to base the results and arrive at some type of conclusion.

In the scenario, threats have been modeled with behaviors that attempt to land at key installation areas in the Port of Oakland. The simulation logic is implemented with counter metric values for each of the threat entities created in each simulation run to capture the status of each threat's attempt to reach the key installation areas. Consolidating these metric values through the "manager objects" in the simulation computes the number of infiltrations which is an example of one of the MOE to be measured. Each of the sensor entities for example: patrol craft, radar sensor, and aircraft have behavior implementation that attempts to interact with the threat entities. There are different kinds of service period for each of the sensor entities. This information is obtained from the analysis of the problem space by the RGTS group. In each simulation run, each sensor entity would interact differently with the threat entities and thus each sensor entity's effectiveness in detecting and eventually deterring the threats are reflected in the difference in the status metric values. In addition, the values of these status metric values are very much affected by the assigned capabilities for the Sensor Entities within the scenario. The utilization of each sensor entity and its ability to detect is computed during each simulation run. At the end of each simulation run, the "manager objects" computes the average utilization, rate of successful detection, rate of classification of targets, and the average time to target detection through the values of the metric values of each sensor entity. From the data that was collected, particular MOE's were analyzed identified prior to the model and simulation aspect. With the data correlated to the particular MOE, statistical information was gathered and linked to the particular alternative. Comparison of the alternatives was solely based on cost because

this issue is the major aspect which all the stakeholders have in common and if time permits further analysis can be conjectured.

The desire of the model is to assist in the MDA of the San Francisco Bay which will assist in the protection of the Port of Oakland. The current system is inadequate to deal with the potential of a waterborne terrorist threat against the Port of Oakland. What the RSTG is hoping to achieve is improved coverage of the area where a potential threat will be addressed in an appropriate manner. That the system will give multiple individuals access to the system and provide awareness to all stakeholders. This awareness aspect will then be operational three hundred and sixty-five days a year, seven days a week and twenty-four hours a day. With this system in place, the cost and benefit will be marginal to the overall effects of a terrorist attack to the Port of Oakland.

Around the Port of Oakland, there are several potential locations that have been identified as vulnerable points where terrorists/threats could potentially launch to attack the vulnerable areas of the port. These areas have been circled in Figure 69. Figure 69 also depicts the routes commonly used by vessels to and from the Pacific Ocean. Figure 70 highlights the key area of the Port of Oakland.

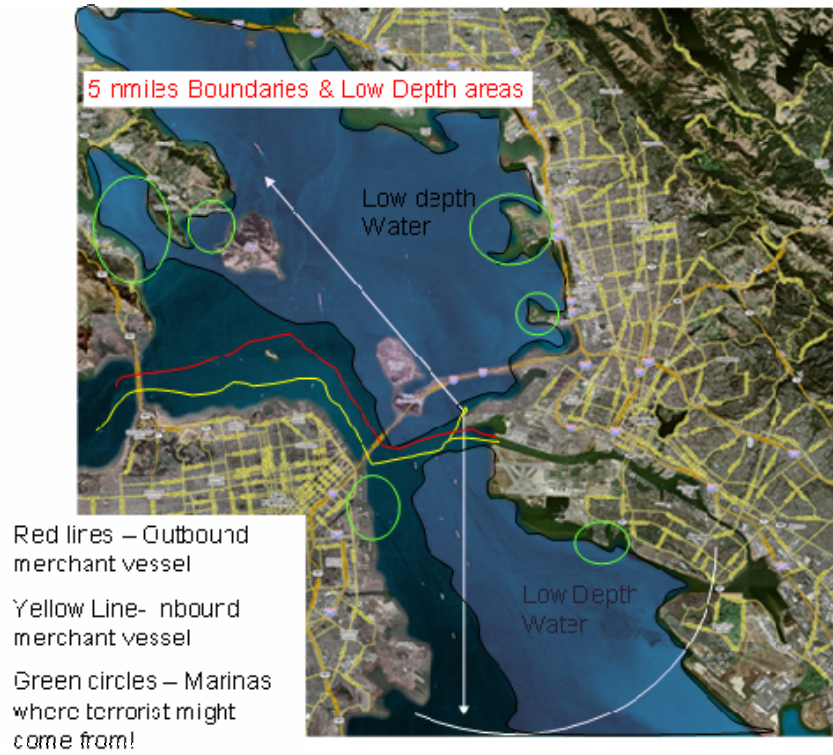


Figure 69. Vulnerable Take Off Point of Terrorist and Vessel Routes



Figure 70. Key Areas of the Port of Oakland

Figures 71 to 76 illustrate six different routes that terrorist/threat entities will be taking off to infiltrate the key areas in the Simulation. Each of these routes originates from different marinas situated in the area of the Port of Oakland.



Figure 71. Route 1 of Threats

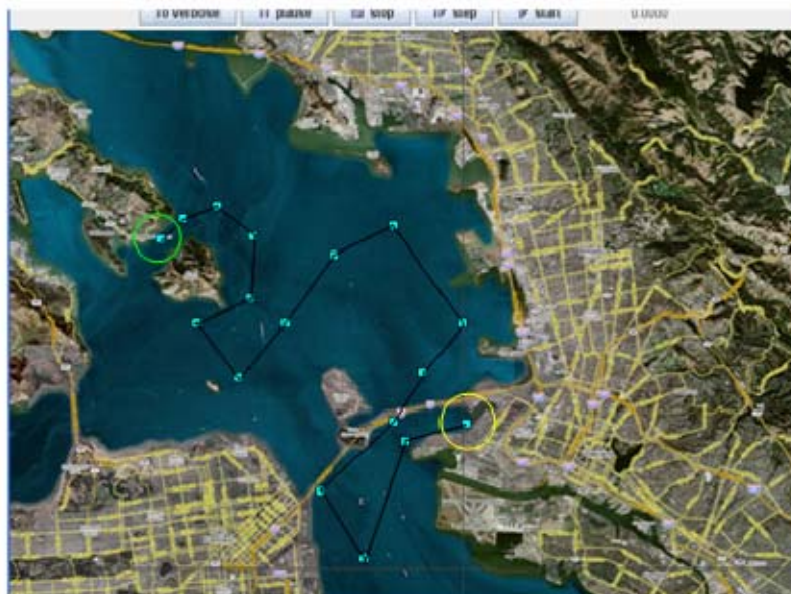


Figure 72. Route 2 of Threats

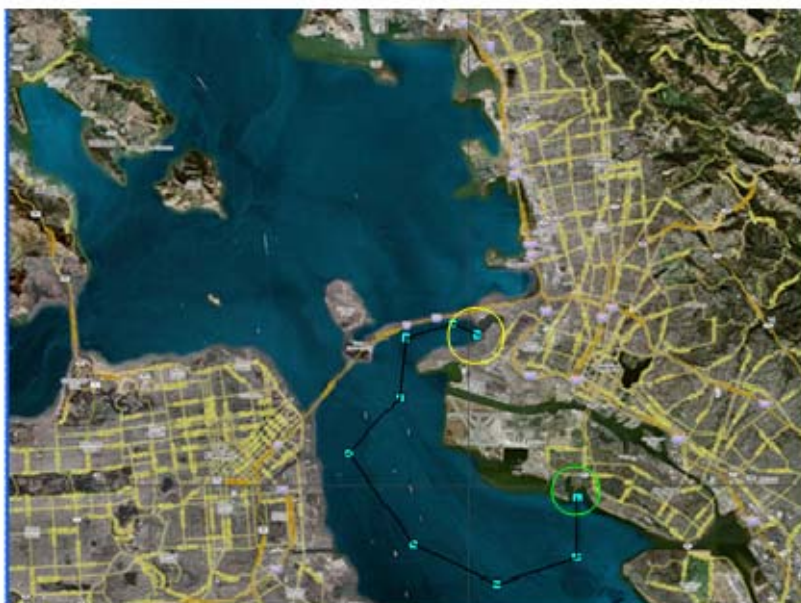


Figure 73. Route 3 of Threats

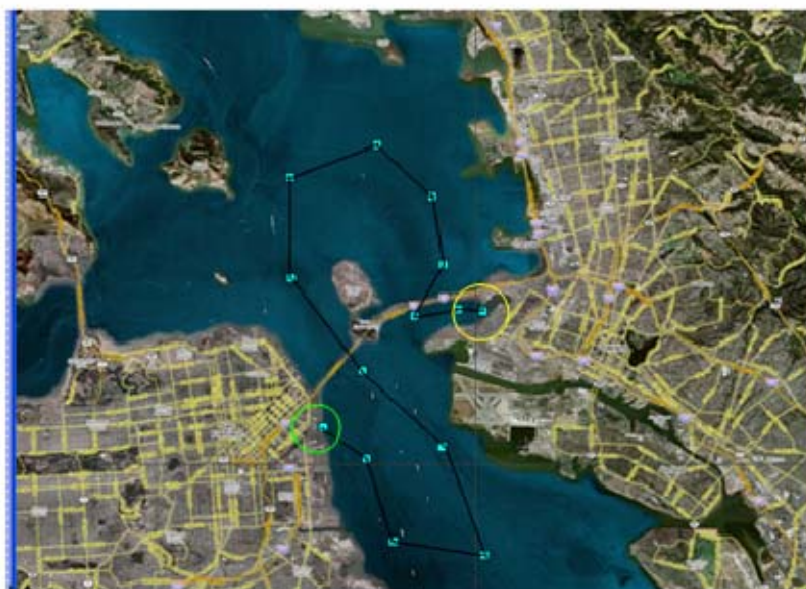


Figure 74. Route 4 of Threats



Figure 75. Route 5 of Threats



Figure 76. Route 6 of Threats

Table 22 lists the sensor specifications encoded in the simulation model:

Patrol Craft		
	Max Speed	10.0 knots
	Max Range	1.0 km
Helo		
	Max Speed	150.0 knots
	Max Range	2.0 km
Scattering non-coherent Radar		
	Max Speed	0.0 knots
	Max Range	2.4 km
ACSR		
(Advanced Coast Surveillance Radar)		
	Max Speed	0.0 knots
	Max Range	5.0 km
Suricate Radar		
	Max Speed	0.0 knots
	Max Range	8.0 km
Giraffe CD Radar		
	Max Speed	0.0 knots
	Max Range	10.0 km
ThermoVision Sentry II		
	Max Speed	0.0 knots
	Max Range	3.0 km
ThermoVision Sentinel		
	Max Speed	0.0 knots
	Max Range	2.6 km
	FOV	10.0 degree
	Directions	{ 250, 70, 250, 110, 80 }
Active OminiDirectional Sonar		
	Max Range	0.15 miles
	Max Speed	0.0 knots
High Frequency Tactical Sonar		
	Max Range	0.5 miles
	Max Speed	0.0 knots
USV		
	Speed	10 knots
	Range	1 km

Table 22. Sensor Specifications Encoded in Port Local Waterside Simulation

Figures 77 and 78 list the encoding of the four routes of the patrol crafts, two routes of the USV and the route of the helicopter. Cyclical route 1 of the patrol craft consists of CG1->CG2->CG3->CG4->CG5->CG6->CG7->CG8->CG9->CG10->CG11->CG12->CG13->CG14->CG15->CG16->CG17->CG18->CG19->CG20->CG4->CG3->CG2->CG1. Cyclical route 2 of the patrol craft is the reverse of cyclical route 1. Cyclical route 3 of the patrol craft consists of CGR3_1->CGR3_2->CGR3_3->CGR3_4->CGR3_5->CGR3_6->CGR3_1. Cyclical route 4 of the patrol craft consists of CGR4_1->CGR4_2->CGR4_3->CGR4_4->CGR4_5->CGR4_6->CGR4_7->CGR4_8->CGR4_1. Cyclical route 1 of the USV consists of USV1->USV2->USV3->USV4->USV5->USV6->USV7->USV8->USV9->USV10->USV11->USV12->USV13->USV14->USV15->USV16->USV17->USV18->USV19->USV3->USV2->USV1. Cyclical route 2 of the USV is the reverse of cyclical route 1. The helicopter flies through the following cyclical route: A1->A2_1->A1->A2_2->A3->A4->A5_1->A4->A5_2->A4->A3->A2_2->A1.

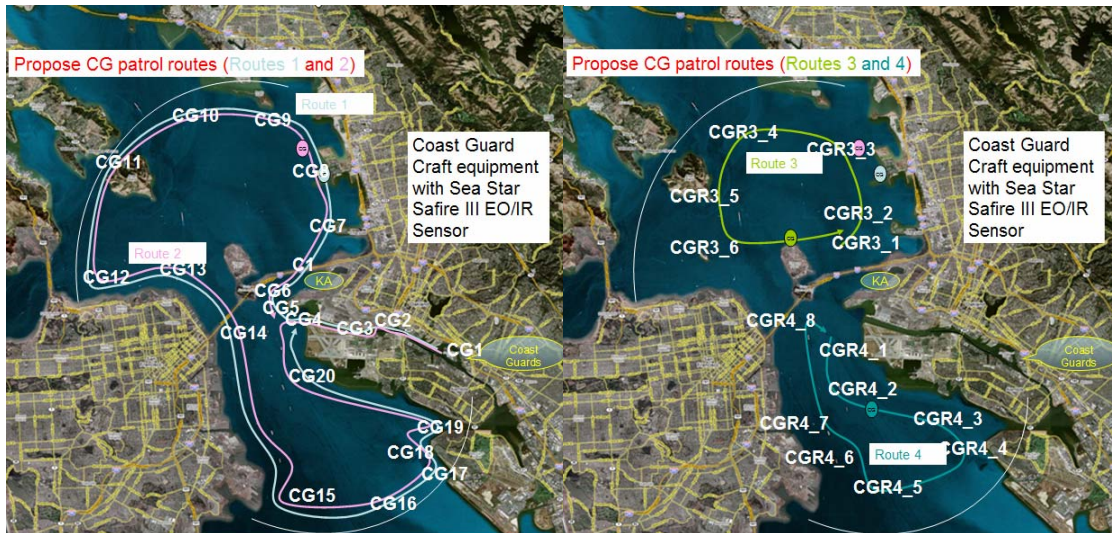


Figure 77. Encoding of Routes of the Patrol Crafts



Figure 78. Encoding of Routes of USV and Helicopter

Figures 79, 80, and 81 show the encoding of the positions of the sensors. R1, R2, and R3 represent the positions of the three radars. TSentry1 and TSentry2 represent the position of the ThermoVision Sentry II sensors. TSent1, TSent2, TSent3, TSent4 and TSent5 represent the position of the five ThermoVision Sentinel sensors. HFTS1, HFTS2, HFTS3, HFTS4 represent the position of the four High Frequency Tactical Sonars. AOS1, AOS2, AOS3, AOS4 and AOS5 represent the position of the five Active OmniDirectional Sonars.



Figure 79. Encoding of Positions and Coverage of the Radars



Figure 80. Encoding of Positions and Coverage of the Electro-Optics Sensors



Figure 81. Encoding of Positions and Coverage of the Acoustic Sensors

4. Simulation Setup

Simulation was performed using the model that was developed by the RSTG by using Simkit. Figure 82 shows the options available for running the simulation. The simulation runs were performed by:

- Executing 30 simulation runs for each specific configuration to obtain a large sample size.
- Varying the types of sensors available for use by the Port of Oakland. These varied from the current suite of sensors available at the Port, as well as those additional alternatives proposed by the team.
- Varying the number of terrorist small boats attempting to reach the Port of Oakland during each simulation run. These numbers varied from 1 to 12, in order evaluate how well the Port could detect the incoming threats.

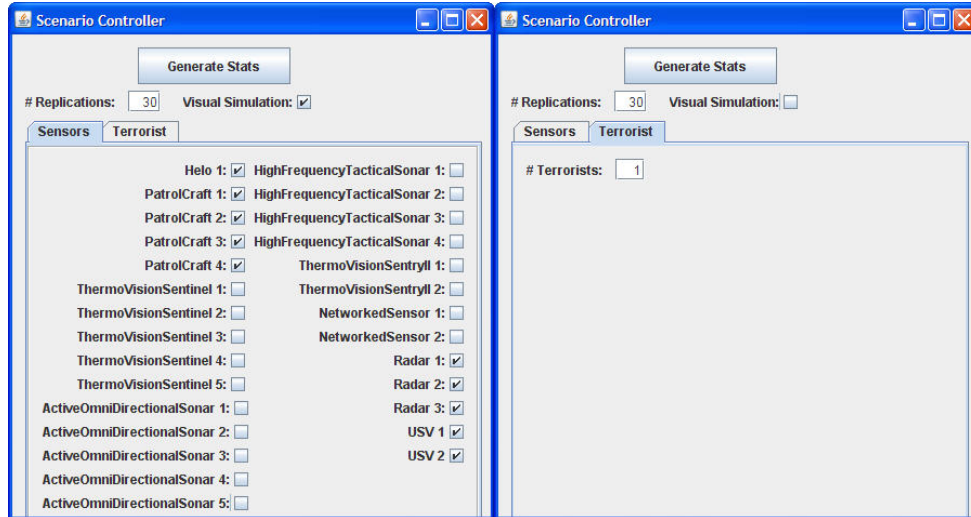


Figure 82. Scenario Controller for Simulation Engine

a. Key Simulation Parameters

Seven possible entry routes for the terrorists were incorporated in the simulation (Six from the various marinas situated in the region near the port, one from the main shipping lane used by ships when they enter the San Francisco Bay). The simulation engine was designed such that each terrorist small boat would randomly select one of these entry routes.

For the transit time along the terrorist routes, the transit typically took between 17 to 30 minutes (depending on their starting locations) to arrive to the destination (which is the key area marked out in the Port of Oakland as shown in Figure 83). The logic behind these routes are that they will normally follow the designated small craft routes, to avoid suspicion, until they are near the port area. The terrorists would then make an abrupt final turn and heading straight for the port.

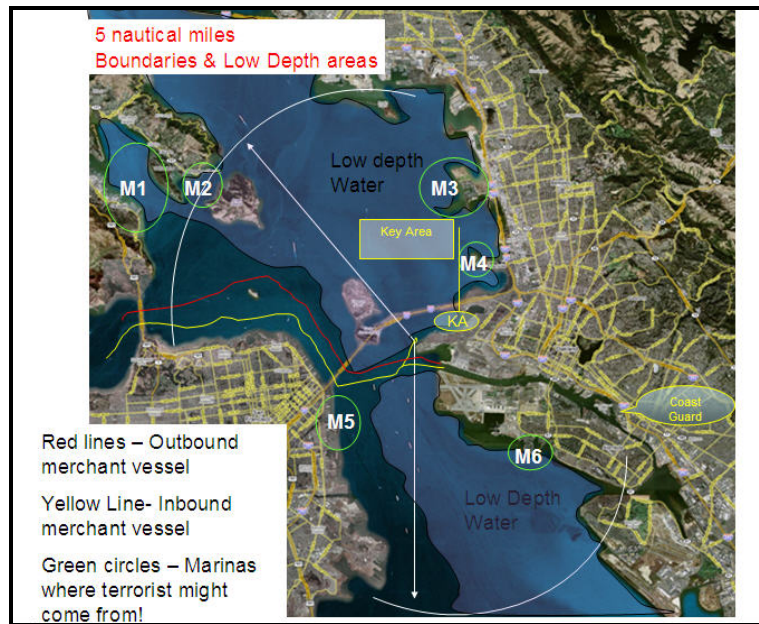


Figure 83. Designated Terrorist Target Area

To enhance the coordination of the attackers, multiple attacker scenarios were simulated such that they all arrived at the scene at once, rather than sequentially to better evaluate the capability of the sensor network to detect and identify multiple threats. Their transit speed was established at 30 knots.

Successful interrogation of a terrorist's small boat was achieved by having each sensor follow a detect-classify-recognize-identify algorithm. The classification, recognition and identification times are each set as three minutes in simulation time. For example, the small boat must be within the coverage of the given sensor for that minimum period before classification/recognition/identification could be achieved by that particular sensor. If the small boat leaves the sensor coverage before the loop is completed, the boat is not successfully interrogated.

The factor of 1:60 is used for conversion between real time and simulation time. For example, one second of real time is equivalent to one min in simulation time.

b. Limitations of the Current Simulation Engine

The assumption was made that when a terrorist's small boat was detected by one of the sensors platforms, it was assumed to be deterred. While this is not necessarily true in any real life situation, this crucial assumption was made to scope the problem to avoid having to deal with the many complexities that arise after detection has occurred (e.g. what to do next, whether to continue tracking or to decide which engagement option to execute). This cannot be easily modeled and requires a human-in-the-loop to decide the next best course of action.

The sensors could only perform single processes for the detection/classification/recognition/identification procedures due to the complexity of encoding this algorithm for multiple targets. The limited time available for the team to build the simulation model from scratch was a major limitation.

The inability of Simkit to model objects moving in three dimensions meant that the implementation of the sonar platforms in this simulation may not correspond to the real world environment. While Diskit, which is an extension of Simkit, allows for 3-D Point (versus Simkit's implementation of Point2D), the team was not confident that the implementation in Diskit would result in a stable simulation engine. Hence, the team reverted to using Simkit, with the associated limitations of Point2D.

c. Simulation Runs

For the simulation runs, different sensor configurations were performed to test the sensor capabilities. These configurations ranged from the RSTG's understanding of the current sensor configuration at the Port of Oakland, to the final configuration that the team proposed. Intermediate configurations were also simulated to gather results to more fully understand the capabilities afforded by the addition or subtraction of any particular set of sensors:

The sensors used are described briefly:

- 1 x Helo The helicopter used by the Coast Guard for use in their Search-And-Rescue (SAR) missions. Detection using this platform is incidental, as it is not primarily deployed as a sensor. Anytime the helicopter was used, only one helicopter was on patrol.

- 4 x Patrol Craft The patrol craft are currently in use by the Coast Guard. It is assumed that a maximum of four of these craft were patrolling the coastal waters around the port at one time. It was assumed that these patrol craft are fitted with the Sea-Star III for improved sensing capability.
- 1 x Radar Configuration This radar is currently in use by the USCG in their daily operations for vessel trafficking service (VTS) not primarily used for port security, it is located at the radar tower located on Yerba Buena Island situated west of the port. It was assumed that this radar has the ability to detect and identify targets with one square meter radar RCS.
- 2 x Radar Configuration In addition to the existing radar, another radar was added to provide wide area sensing and target tracking. The additional radar needed not necessarily be able to detect targets with a one square meter RCS.
- 3 x Radar Configuration In addition to the existing radar, two additional radars were being implemented for wide area sensing and target tracking. These additional radars needed not necessarily be able to detect targets with the one square meter RCS.
- 2 x Unmanned Surface Vehicles The PROTECTOR Class USVs were proposed to complement the manned patrols. They may be used for routine patrolling as well as any interdiction operations.
- 2 x Thermo Vision SentryII The Thermo Vision Sentry II aided in providing continuous wide area high resolution thermal imaging.
- 5 x Thermo Vision Sentinel The Thermo Vision Sentinel aided in providing continuous focused-view high resolution thermal imaging for perimeter-sensing for the port.
- 2 x Networked Sensor The Networked Sensors were a vertical array of passive receivers that were deployed in shallow water and supported by surface buoys.
- 5 x Active Omni Directional Sonar The Active Omni Directional Sonar was primarily used for the detection of subsurface threats. While the perceived main threat in this case was from small boat attacks, the possibility of a subsurface threat remained. Furthermore, sonar could also detect the perturbations caused by fast approaching small craft. Hence, the sonar was included.

- 4 x High Frequency Tactical Sonar Similar to the Active Omni Directional Sonars, the High Frequency Tactical Sonar were also used for the detection of potential subsurface threats.

The sensor configurations (column headings) and type of sensor platforms (row headings) are summarized in Table 23.

Sensor Configuration Type of Sensor Platform	(A) Current	(B) (A) + USV	(C) (B) + 1 Radar	(D) (B) + 2 Radars	(E) (D) + SentryII	(F) (E) + Sentinel	(G) (F) + Buoys + Sonars
1 x Helo	✓	✓	✓	✓	✓	✓	✓
4 x Patrol Craft	✓	✓	✓	✓	✓	✓	✓
1 x Radar Configuration (Existing)	✓	✓					✓
2 x Radar Configuration			✓				✓
3 x Radar Configuration				✓	✓	✓	✓
2 x Unmanned Surface Vessels (USV)		✓	✓	✓	✓	✓	✓
2 x ThermoVisionSentryII					✓	✓	✓
5 x ThermoVisionSentinel						✓	✓
2 x Networked Sensor (Buoys)							✓
5 x Active OmniDirectional Sonar							✓
4 x High Frequency Tactical Sonar							✓

Table 23. RSTG Sensor and Platform Configurations for Simulation

5. Results and Key Findings

a. Current Configuration

Based on interviews and conversations with the Port of Oakland and the USCG, the current sensor configuration for the Port of Oakland was assumed to be the following:

- 1 Helo
- 4 Patrol Crafts
- 1 Radar (situated on Yerba Buena Island)

This was the assumed current configuration for the Port of Oakland; it was the baseline configuration for which the other configurations will be compared against in terms of how the added sensors and platforms would increase the detection capability.

Table 24 and Figure 84 summarized the detection and infiltration rates of the simulation runs with the varying numbers of terrorist small boats:

# of Terrorist Small Boats	% Infiltration	% Detection
1	16.67%	83.33%
2	33.33%	66.67%
3	41.11%	58.89%
4	48.33%	51.67%
5	54.00%	46.00%
6	61.67%	38.33%
9	71.11%	28.89%
12	76.94%	23.06%

Table 24. Infiltration and Detection Rate for (A) Configuration

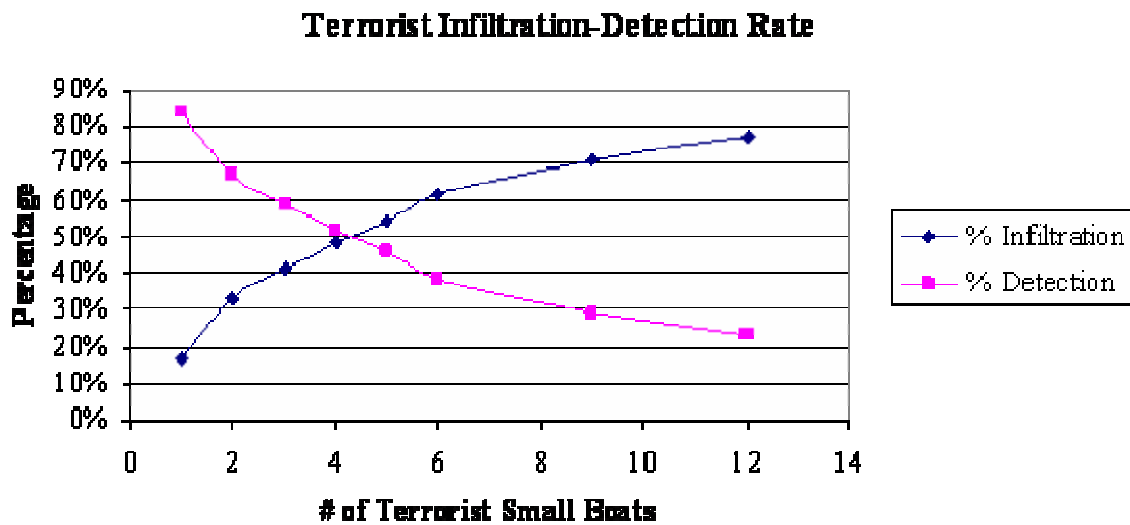


Figure 84. Infiltration and Detection Rate for (A) Configuration

With regards to Table 25, the detection rate is defined as the number of contacts that were successfully interrogated by completing the classification/recognition/identification chain.

The detection rate by the respective sensors is summarized in Table 25:

Sensor	Detection Rate for given number of Terrorist Small Boats							
	1	2	3	4	5	6	9	12
Helo	0	0	0	0	0	0	0	0
Patrol Craft 1	1	7	9	10	12	20	18	28
Patrol Craft 2	0	0	2	4	5	3	5	7
Patrol Craft 3	3	5	11	16	19	14	22	23
Patrol Craft 4	0	1	1	2	3	2	3	10
Radar 1	21	27	30	30	30	30	30	30
Undetected	5	20	37	58	81	111	192	277
Total	30	60	90	120	150	180	270	360

Table 25. Sensor Detection Rate for (A) Configuration

b. Current and USV (B)

The simulation runs with this sensor configuration sought to verify the increased capability afforded by the addition of Unmanned Surface Vessels. The configuration was modeled by including the following:

- 1 Helo
- 4 Patrol Crafts
- 1 Radar
- 2 USVs

Table 26 and Figure 85 summarized the detection and infiltration rates of the simulation runs with the varying numbers of terrorist small boats:

# of Terrorist Small Boats	% Infiltration	% Detection
1	16.67%	83.33%
2	20.00%	80.00%
3	28.89%	71.11%
4	30.83%	69.17%
5	43.33%	56.67%
6	45.00%	55.00%
9	58.89%	41.11%
12	65.28%	34.72%

Table 26. Infiltration and Detection Rate for (B) Configuration

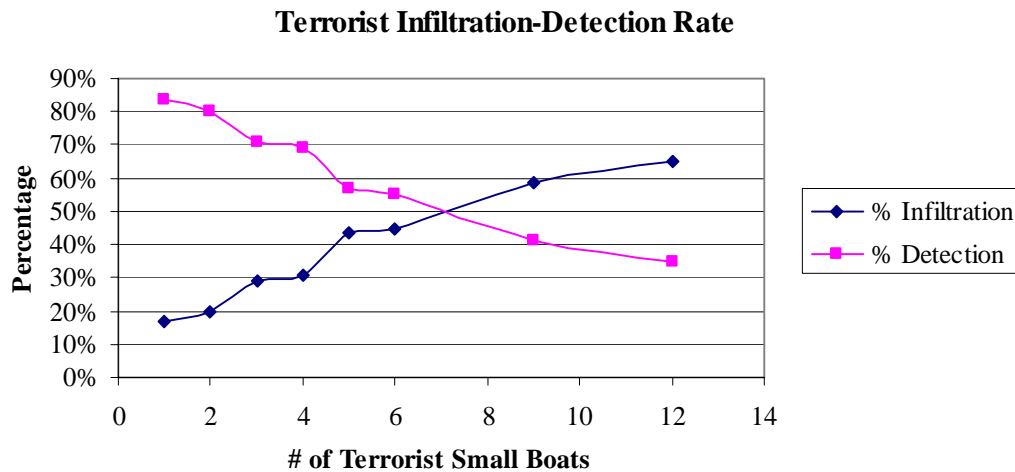


Figure 85. Infiltration and Detection Rate for (B) Configuration

The detection rates by the respective sensors were summarized in the Table 27:

Sensor	Detection Rate for given number of Terrorist Small Boats							
	1	2	3	4	5	6	9	12
Helo	0	0	0	0	0	0	0	0
Patrol Craft 1	5	1	4	10	10	10	17	16
Patrol Craft 2	0	1	0	2	3	2	3	5
Patrol Craft 3	5	7	8	13	17	18	20	25
Patrol Craft 4	0	1	0	1	0	2	2	4
Radar 1	11	23	29	28	29	29	30	30
USV 1	3	10	14	19	13	18	22	21
USV 2	1	5	9	10	13	20	17	24
Undetected	5	12	26	37	65	81	159	235
Total	30	60	90	120	150	180	270	360

Table 27. Sensor Detection Rate for (B) Configuration

c. Current and USV and 1 Additional Radar (C)

The simulation runs with this sensor configuration sought to verify the increased capability afforded by the addition of a wide-area sensing radar with tracking capability. The modeled configuration was as follows:

- 1 Helo
- 4 Patrol Crafts
- 2 Radars
- 2 USVs

Table 28 and Figure 86 summarized the detection and infiltration rates of the simulation runs with varying the numbers of terrorist small boats.

# of Terrorist Small Boats	% Infiltration	% Detection
1	0	100
2	3.33	96.67
3	6.67	93.33
4	13.33	86.67
5	24	76
6	35.56	64.44
9	51.48	48.52
12	58.33	41.67

Table 28. Infiltration and Detection Rate for (C) Configuration

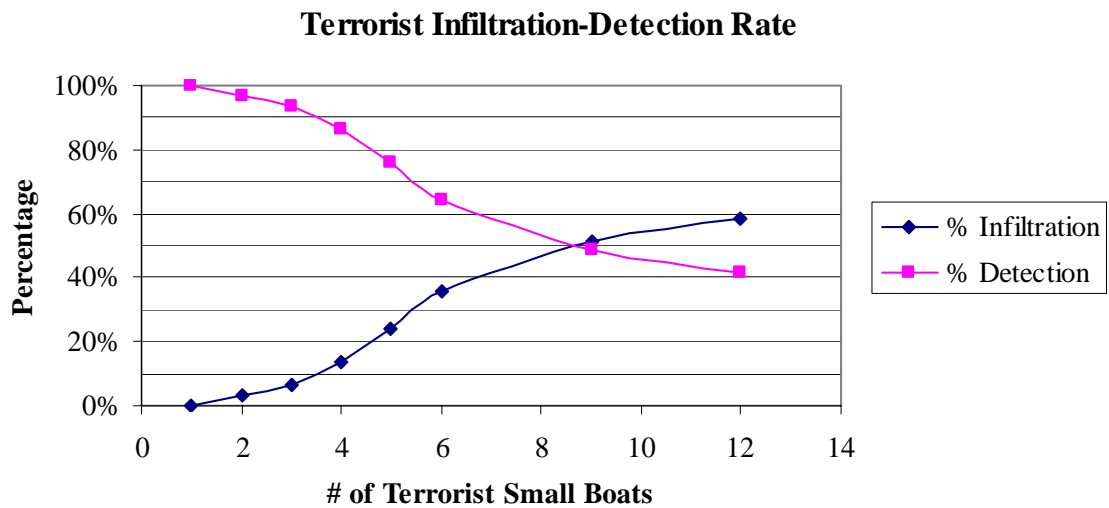


Figure 86. Infiltration and Detection Rate for (C) Configuration

The detection rate by the respective sensors is shown in Table 29.

Sensor	Detection Rate for given number of Terrorist Small Boats							
	1	2	3	4	5	6	9	12
Helo	0	0	0	0	0	0	0	0
Patrol Craft 1	0	0	3	9	14	8	19	19
Patrol Craft 2	0	0	1	2	1	2	5	4
Patrol Craft 3	0	0	2	6	6	9	9	19
Patrol Craft 4	2	0	2	2	2	2	3	2
Radar 1	4	22	27	28	30	30	30	30
Radar 2	22	27	30	30	29	30	30	30
USV 1	1	7	12	17	13	18	17	18
USV 2	1	2	7	10	19	17	18	28
Undetected	0	2	6	16	36	64	139	210
Total	30	60	90	120	150	180	270	360

Table 29. Sensor Detection Rate for (C) Configuration

d. Current and USV and 2 Additional Radar (D)

The simulation runs with this sensor configuration sought to verify the increased capability afforded by the addition of two wide-area sensing radars with tracking capability. The modeled configuration was:

- 1 Helo
- 4 Patrol Crafts
- 3 Radars
- 2 USVs

Table 30 and Figure 87 summarized the detection and infiltration rates of the simulation runs with varying the numbers of terrorist small boats:

# of Terrorist Small Boats	% Infiltration	% Detection
1	0.00%	100.00%
2	0.00%	100.00%
3	4.44%	95.56%
4	3.33%	96.67%
5	14.00%	86.00%
6	19.44%	80.56%
9	42.96%	57.04%
12	50.56%	49.44%

Table 30. Infiltration and Detection Rate for (D) Configuration

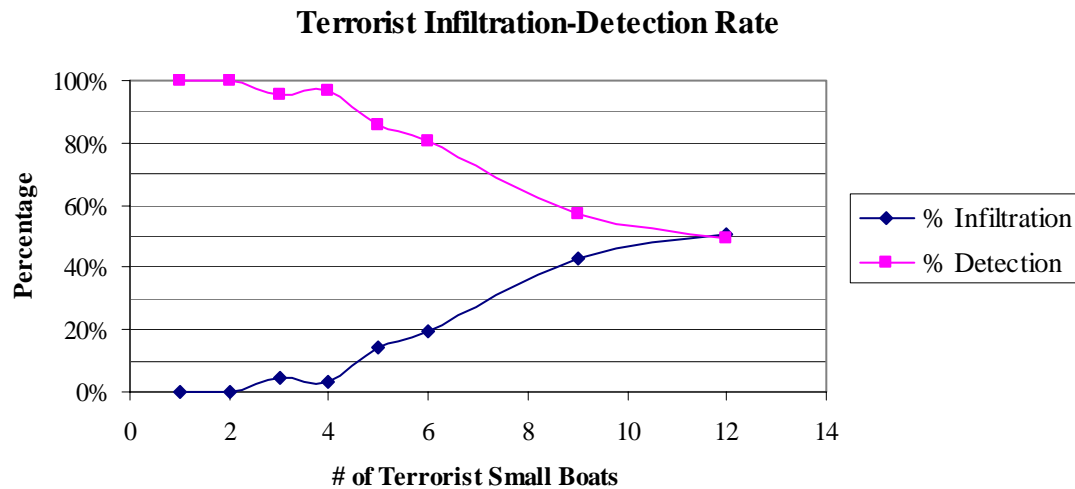


Figure 87. Infiltration and Detection Rate for (D) Configuration

The detection rates of the respective sensors were summarized in Table

31.

Sensor	Detection Rate for given number of Terrorist Small Boats							
	1	2	3	4	5	6	9	12
Helo	0	0	0	0	0	0	0	0
Patrol Craft 1	0	0	2	4	6	12	15	23
Patrol Craft 2	0	0	0	1	1	1	3	3
Patrol Craft 3	0	0	2	1	7	10	9	15
Patrol Craft 4	0	0	0	1	2	1	4	4
Radar 1	0	6	21	27	26	30	30	30
Radar 2	22	25	28	29	29	28	30	30
Radar 3	8	29	30	30	30	30	30	30
USV 1	0	0	2	12	14	19	17	21
USV 2	0	0	1	11	14	14	16	22
Undetected	0	0	4	4	21	35	116	182
Total	30	60	90	120	150	180	270	360

Table 31. Sensor Detection Rate for D Configuration

e. Current and USV and 2 Additional Radar and Thermo Vision Sentry II (E)

The simulation runs with this sensor configuration sought to verify the increased capability afforded by the addition of two wide-area sensing radars with tracking capability. The modeled configuration was:

- 1 Helo
- 4 Patrol Crafts
- 3 Radars
- 2 USVs
- 2 Thermo Vision Sentry II

Table 32 and Figure 88 summarized the detection and infiltration rates of the simulation runs with the varying numbers of terrorist small boats:

# of Terrorist Small Boats	% Infiltration	% Detection
1	0.00%	100.00%
2	0.00%	100.00%
3	0.00%	100.00%
4	10.00%	90.00%
5	14.00%	86.00%
6	25.56%	74.44%
9	37.04%	62.96%
12	46.11%	53.89%

Table 32. Infiltration and Detection Rate for (E) Configuration

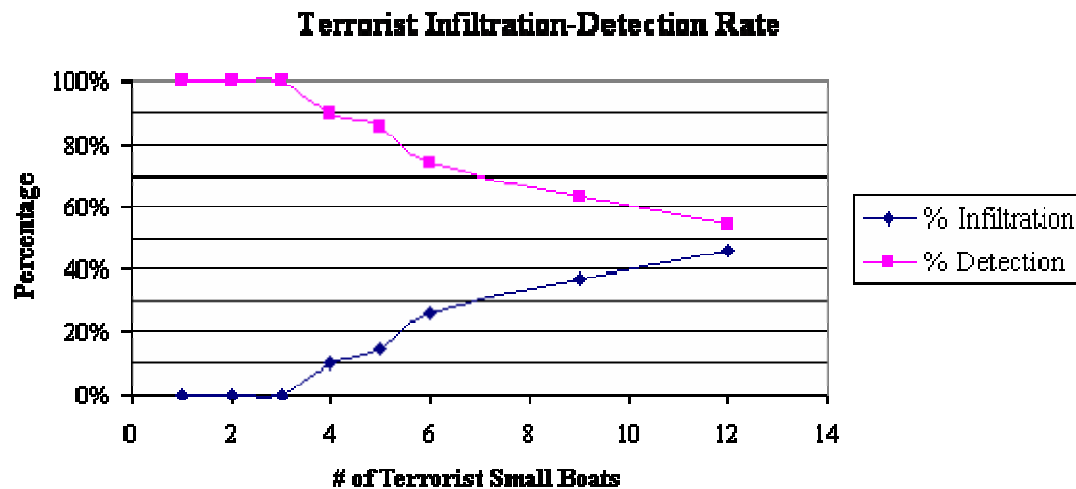


Figure 88. Infiltration and Detection Rate for (E) Configuration

The detection rates of the respective sensors were summarized in Table 33.

Sensor	Detection Rate for given number of Terrorist Small Boats							
	1	2	3	4	5	6	9	12
Helo	0	0	0	0	0	0	0	0
Patrol Craft 1	0	0	1	3	6	5	9	23
Patrol Craft 2	0	0	0	0	1	1	2	3
Patrol Craft 3	0	0	2	3	7	6	10	17
Patrol Craft 4	0	0	0	0	1	2	1	3
Radar 1	0	1	16	17	27	26	30	30
Radar 2	26	22	26	26	29	30	30	30
Radar 3	4	30	30	30	29	30	30	30
USV 1	0	0	2	5	7	7	20	13
USV 2	0	0	0	6	6	8	14	19
ThermoVisionSentryII 1	0	7	13	18	16	19	24	26
ThermoVisionSentryII 2	0	0	0	0	0	0	0	0
Undetected	0	0	0	12	21	46	100	166
Total	30	60	90	120	150	180	270	360

Table 33. Sensor Detection Rate for E Configuration

f. Current and USV and 2 Additional Radar and Thermo Vision Sentry II and Thermo Vision Sentinel (F)

The simulation runs with this sensor configuration sought to verify the increased capability afforded by the addition of two wide-area sensing radars with tracking capability. The modeled configuration was:

- 1 Helo
- 4 Patrol Crafts
- 3 Radars
- 2 USVs
- 2 Thermo Vision Sentry II
- 5 Thermo Vision Sentinel

Table 34 and Figure 89 summarized the detection and infiltration rates of the simulation runs with varying the numbers of terrorist small boats:

# of Terrorist Small Boats	% Infiltration	% Detection
1	0.00%	100.00%
2	0.00%	100.00%
3	0.00%	100.00%
4	5.00%	95.00%
5	9.33%	90.67%
6	12.22%	87.78%
9	29.26%	70.74%
12	41.11%	58.89%

Table 34. Infiltration and Detection Rate for (F) Configuration

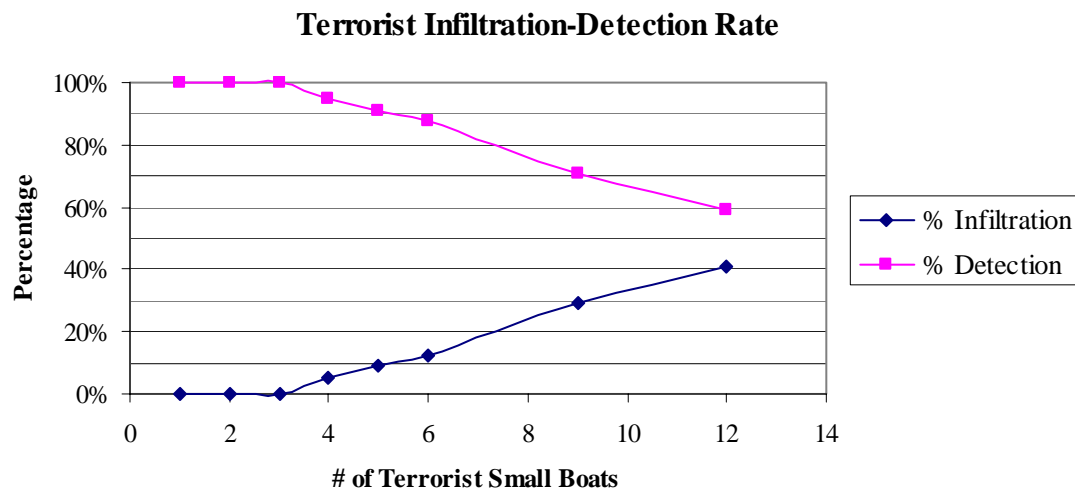


Figure 89. Infiltration and Detection Rate for (F) Configuration

The detection rates of the respective sensors were summarized in Table 35.

Sensor	Detection Rate for given number of Terrorist Small Boats							
	1	2	3	4	5	6	9	12
Helo	0	0	3	0	0	0	0	0
Patrol Craft 1	0	0	3	3	6	6	12	16
Patrol Craft 2	0	0	3	0	1	2	2	1
Patrol Craft 3	0	0	1	2	6	3	16	12
Patrol Craft 4	0	0	3	1	0	1	2	4
Radar 1	0	2	14	17	17	29	29	30
Radar 2	15	24	28	29	29	29	30	30
Radar 3	15	28	30	30	30	30	30	30
USV 1	0	0	1	4	14	13	15	13
USV 2	0	0	1	3	4	9	9	11
ThermoVisionSentryII 1	0	0	15	14	17	17	21	23
ThermoVisionSentryII 2	0	6	3	0	0	0	1	0
ThermoVisionSentinel 1	0	0	3	10	11	13	17	21
ThermoVisionSentinel 2	0	0	3	0	0	0	0	0
ThermoVisionSentinel 3	0	0	3	1	1	6	7	16
ThermoVisionSentinel 4	0	0	3	0	0	0	0	0
ThermoVisionSentinel 5	0	0	3	0	0	0	0	0
Undetected	0	0	3	6	14	22	79	148
Total	30	60	90	120	150	180	270	360

Table 35. Sensor Detection Rate for F Configuration

g. Current and USV and 2 Additional Radar and Thermo Vision Sentry II and Thermo Vision Sentinel and Networked Sensors and Sonar (F)

The simulation runs on this sensor configuration sought to verify the increased capability afforded by the addition of Networked Sensors supported by buoys, as well as sonar. The modeled configuration was:

- 1 Helo
- 4 Patrol Crafts
- 3 Radars
- 2 USVs
- 2 Thermo Vision Sentry II
- 5 Thermo Vision Sentinel
- 2 Networked Sensors
- 5 Active Omni Directional Sonar
- 4 High Frequency Tactical Sonar

Table 36 and Figure 90 summarized the detection and infiltration rates of the simulation runs with varying the numbers of terrorist small boats.

# of Terrorist Small Boats	% Infiltration	% Detection
1	0.00%	100.00%
2	0.00%	100.00%
3	0.00%	100.00%
4	4.17%	95.83%
5	8.00%	92.00%
6	9.44%	90.56%
9	25.56%	74.44%
12	37.50%	62.50%

Table 36. Infiltration and Detection Rate for (G) Configuration

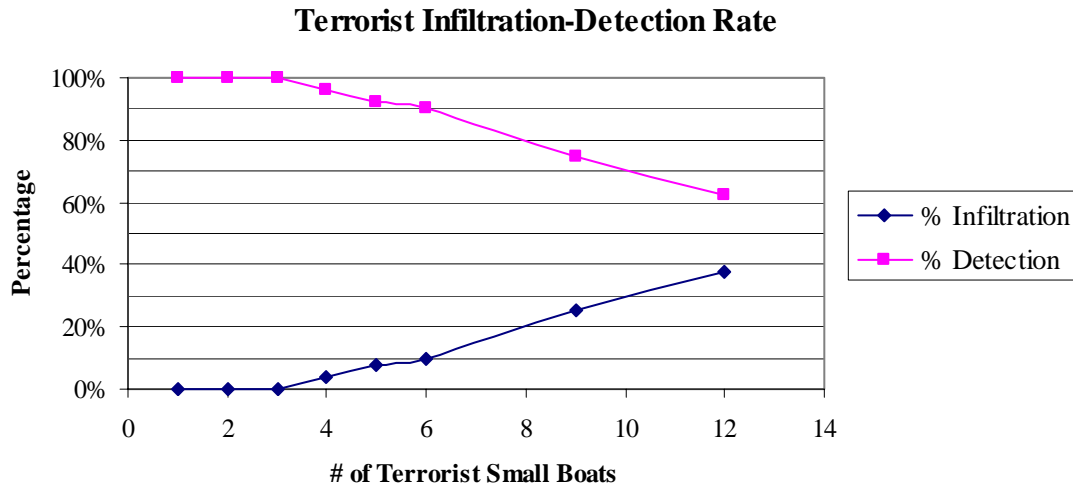


Figure 90. Infiltration and Detection Rate for (G) Configuration

The detection rates of the respective sensors were summarized in Table 37.

Sensor	Detection Rate for given number of Terrorist Small Boats							
	1	2	3	4	5	6	9	12
Helo	0	0	0	0	0	0	0	0
Patrol Craft 1	0	0	0	2	3	4	7	9
Patrol Craft 2	0	1	0	0	0	1	2	3
Patrol Craft 3	0	0	1	4	4	4	11	14
Patrol Craft 4	0	0	0	1	0	1	0	1
Radar 1	0	0	9	15	20	27	28	30
Radar 2	16	26	27	28	28	29	30	30
Radar 3	14	27	30	30	30	30	30	30
USV 1	0	2	3	4	4	9	12	14
USV 2	0	1	2	2	4	7	11	13
Networked Sensor 1	0	0	0	0	1	1	2	4
Networked Sensor 2	0	0	0	0	1	2	2	3
ThermoVisionSentinel 1	0	1	3	8	13	15	17	18
ThermoVisionSentinel 2	0	0	0	0	0	0	0	0
ThermoVisionSentinel 3	0	1	3	5	9	10	15	17
ThermoVisionSentinel 4	0	0	0	0	0	0	0	0
ThermoVisionSentinel 5	0	0	0	0	0	0	0	0
ThermoVisionSentryII 1	0	1	12	16	19	20	23	26
ThermoVisionSentryII 2	0	0	0	0	0	0	0	0
Active Omni Directional Sonar 1	0	0	0	0	0	0	3	4
Active Omni Directional Sonar 2	0	0	0	0	2	3	4	3
Active Omni Directional Sonar 3	0	0	0	0	0	0	1	1
Active Omni Directional Sonar 4	0	0	0	0	0	0	3	3
Active Omni Directional Sonar 5	0	0	0	0	0	0	0	2
High Frequency Tactical Sonar 1	0	0	0	0	0	0	0	0
High Frequency Tactical Sonar 2	0	0	0	0	0	0	0	0
High Frequency Tactical Sonar 3	0	0	0	0	0	0	0	0
High Frequency Tactical Sonar 4	0	0	0	0	0	0	0	0
Undetected	0	0	0	5	12	17	69	135
Total	30	60	90	120	150	180	270	360

Table 37. Sensor Detection Rate for G Configuration

h. Key Findings

A simultaneous comparison of the results is shown in Figure 91 below.

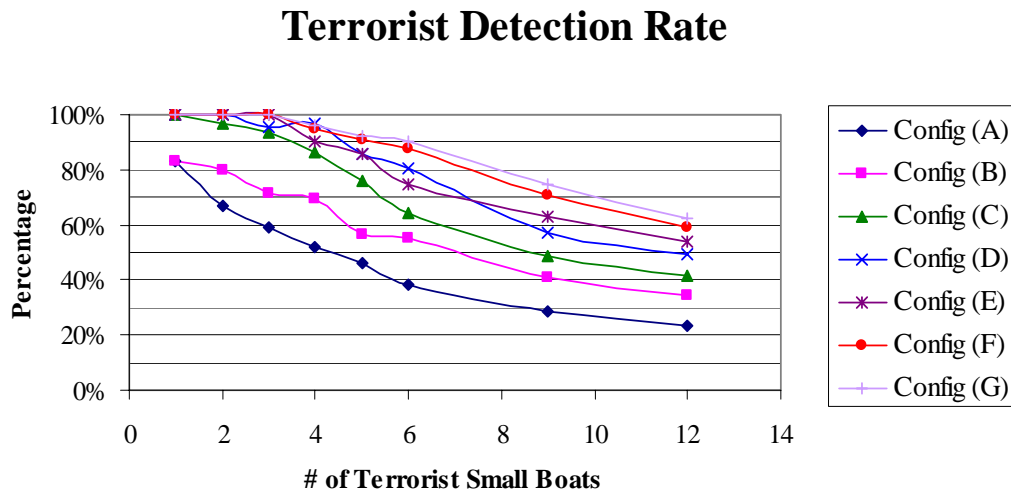


Figure 91. Terrorist Detection Rate for Various Sensor Configurations

While the detection rates decreased as the number of terrorist small boats increased, it is noticed that the rate of reduction is smaller with a multi-layered system. This is primarily due to the RSTG’s assessment that the optimal sensor solution should be a multi-layered sensor plan. This is vital in ensuring that the various sensor platforms form an effective network to detect against incoming threats.

While the detection rate seems to decrease with the increasing number of terrorist small boats, RSTG realized that this could be due to the limitations of the simulation engine that was used. More specifically, each sensor platform could only detect a single target at any one time. The lengthy classification/recognition/identification process for any target usually resulted in the other targets being able to ‘escape’ detection from the same sensor. This further reinforces the necessity for the Port of Oakland to adopt a multi-layered sensor architecture for effective target interrogation.

While real operational sensors could perform multiple threat detection and tracking, the many uncertainties present in reality can result in the sensor suite not being used to its full potential. This may not enable for appropriate counter terrorist operations to be performed within the limited time before the terrorist is able to reach his objective.

The performance of the various sensor platforms are summarized as follows:

- Radars - Radars form the first line of detection. This is due to their wide-area sensing capabilities, and their respective detection times confirm that they are the first to detect incoming targets.
- EO/IR Sensors - The suite of Thermo Vision sensors that provided EO/IR sensing capabilities were also useful in detecting the incoming threats that managed to 'evade' radar detection
- Helo - Helicopters, primarily used for SAR operations, are not very useful in detecting targets in this simulation. However, in real life, their ability to move from location to location at high speeds among the shipping vessels gives them a distinct advantage should the need arise for the USCG to get from place to place quickly.
- Patrol Craft - While the detection rates of the patrol craft may appear to be small compared to other sensor platforms like the radars, their importance in reality cannot be overstated. While the detection of terrorists would be incidental (i.e. being at the right place at the right time), their very presence in the waters surrounding the port serves to deter any potential attackers, and this deterrence is a viable form of defense.
- USVs - USVs are similar to patrol craft in that their 'detection' of terrorists would also be incidental. However, like patrol craft, their very presence in the waters serve to deter any potential attackers. Furthermore, the ability to use these unmanned vessels for interdiction in hazardous scenarios could often save the lives of the security personnel who would otherwise have to confront any hostile elements.
- Networked Sensor - Networked Sensors, using buoys, did not seem to be particularly useful in the simulation, as demonstrated by their low detection rates. Their small coverage areas meant that they will be triggered only if there is disturbance right in the immediate vicinity of the mounted sensor. Furthermore, although not simulated, it is expected that the power requirements of these Networked Sensors would be difficult to support.
- Sonar - Sonar did not seem particularly useful in the simulation demonstrated by their low detection rates. This is largely due to the fact that the primary perceived threat was from surface attacks by small boats, and hence the simulation was modeled that way. Sonar

could possibly be useful in the detection of subsurface threats, and ought to be considered for those threats.

5. Cost Estimation

The RSTG gathered cost estimation data for the alternatives that provided the waterborne defense against the small boat threat to the Port of Oakland. This data was used to conduct a cost benefit analysis of the alternatives. The cost benefit analysis illustrates the amount of anticipated performance that could be achieved for a given cost and which alternative provides the most effectiveness for the associate cost. More simply stated, the objective is to show a graphical representation of the “bang for the buck” amongst the alternatives. The RSTG cost estimation did not examine the application of these alternatives inside the individual terminals of to the Port of Oakland. This option was deemed too costly and infeasible. What the RSTG examined was the application of the alternatives to the assets that are already in place in regards to the mission of port security. These assets mainly belong to the USCG, which is tasked with the job of port security and directly involved in the protection of the Port of Oakland.

All costs are in 2007 U.S. Dollars (USD) and were acquired from corresponding with sales associates and operators of the various systems and required equipment. Life cycle cost estimates included procurement cost and operational and support aspects of the required equipment. This provided a reasonable value for the total cost of each of the alternatives which mainly focused on the acquisition and ownership of the equipment. The term sunk cost is the money already paid for a particular asset for MDA. Due to the time frame of the PSS12 project, research and development cost; disposal cost; as well as any upgrades were not calculated and figured into the cost estimation.

Cost estimation is based on historical data. Based on that basic principle the operational and support costs that is not provided by vendors or operators was based on the rule of thumb that 30 to 70 percent of the procurement cost is the typical annual operation and support costs. Again, the following are purely estimates obtained through calculations and conversations and should not be considered the actual procurement and O&S costs.

Special note must be addressed upon the cost of the USVs selected. This applies to all configurations except for the current configuration. With this particular type of USV, a large portion of the total cost is contributed to procurement and O&S of two USVs. The cost encompasses a boat, trailer, gun mount (7.62 mm, mini-Typhoon), Toplight (EO/IR) system, spare kit, control station (two person), on site training and warranty. Different USV platforms are out on the market and cost not nearly as much but because of the Protector's proven performance out in the fleet and diverse mission roles it was assumed the best candidate for the mission of port security. Table 38 depicts the cost of the various alternatives.

Alternatives	FY07 Cost
A	\$4,140,000.00
B	\$14,640,000.00
C	\$17,890,000.00
D	\$21,140,000.00
E	\$21,312,000.00
F	\$21,448,000.00
G	\$46,648,000.00

Table 38. Summary of Cost per Configuration

Current Configuration (A)

With the current configuration a large portion of the total cost has already been paid for from previous fiscal year budgets. This is common referred to as sunk cost. For example, if USCG already has four SAFE Boats in operation, there is not a need to repurchase the boats. What remains is the operational and support (O&S) costs for maintaining and support the missions of the particular assets. Table 39 represents the procurement costs, quantity, and O&S costs.

	Est. Procurement Cost	Quantity	Sunk Cost	O&S Cost
Manned aircraft (HH-65C)	\$8,800,000.00	1	\$8,800,000.00	\$3,520,000.00
ship (SAFE Boats)	\$200,000.00	4	\$800,000.00	\$320,000.00
X-Band	\$1,000,000.00	1	\$1,000,000.00	\$300,000.00
			Total FY07 cost	\$4,140,000.00

Table 39. Total Cost for Alternative A

Current + USV (B)

With this configuration, the addition of an USV was used in the cost estimation. The Protector is used and was the only USV examined because of its diverse mission profile and its legitimate functional role in port security. The high procurement cost comes from the many different amenities that come along with the baseline version of the Protector. In regards to the model, RSTG used two USVs and therefore USV procurement was added to the total cost. Table 40 represents the procurement costs, quantity, and O&S costs.

	Est. Procurement Cost	Quantity	Sunk Cost	Procurement Cost	O&S Cost
Manned aircraft (HH-65C)	\$8,800,000.00	1	\$8,800,000.00	\$0.00	\$3,520,000.00
Ship (SAFE Boats)	\$200,000.00	4	\$800,000.00	\$0.00	\$320,000.00
X-Band	\$1,000,000.00	1	\$1,000,000.00	\$0.00	\$300,000.00
USV (Protector)	\$3,500,000.00	2		\$7,000,000.00	\$3,500,000.00
				\$7,000,000.00	\$7,640,000.00
				Total FY07 cost	\$14,640,000.00

Table 40. Total Cost for Alternative B

Current + USV + One Additional Radar (C)

With this configuration, an additional X-Band Radar was procured and used in conjunction with the items in configuration B. O&S costs for the Suricate X- Band radar was determined by analogy to the existing X-Band radar. Using the O&S percentage of the existing X-Band radar and applying it to the procurement cost of the Suricate radar, the O&S cost of the Suricate X-Band radar was determined as indicated in Table 41.

	Est. Procurement Cost	Quantity	Sunk Cost	Procurement Cost	O&S Cost
Manned aircraft (HH-60C)	\$8,800,000.00	1	\$8,800,000.00	\$0.00	\$3,520,000.00
ship (SAFF Bnats)	\$200,000.00	4	\$800,000.00	\$0.00	\$320,000.00
X-Band	\$1,000,000.00	1	\$1,000,000.00	\$0.00	\$300,000.00
X-Band(Suricate)	\$2,500,000.00	1		\$2,500,000.00	\$750,000.00
USV (Protector)	\$3,500,000.00	2		\$7,000,000.00	\$3,500,000.00
				\$9,500,000.00	\$8,390,000.00
				Total FY07 cost	\$17,890,000.00

Table 41. Total Cost for Alternative C

Current + USV + Two Additional Radars (D)

The same procedure described previously was with this alternative. In this configuration, an additional Suricate radar was used. Table 42 summarizes the total cost for this alternative.

	Est. Procurement Cost	Quantity	Sunk Cost	Procurement Cost	O&S Cost
Manned aircraft (HH-65C)	\$8,800,000.00	1	\$8,800,000.00	\$0.00	\$3,520,000.00
ship (SAFE Boats)	\$200,000.00	4	\$800,000.00	\$0.00	\$320,000.00
X-Band	\$1,000,000.00	1	\$1,000,000.00	\$0.00	\$300,000.00
X-Band(Suricate)	\$2,500,000.00	2		\$5,000,000.00	\$1,500,000.00
USV (Protector)	\$3,500,000.00	2		\$7,000,000.00	\$3,500,000.00
				\$12,000,000.00	\$9,140,000.00
				Total FY07 cost	\$21,140,000.00

Table 42. Total Cost for Alternative D

Current + USV + Two Additional Radar + Thermo Vision Sentry II (E)

Table 43 summarizes the total cost for alternative E.

	Est. Procurement Cost	Quantity	Sunk Cost	Procurement Cost	O&S Cost
Manned aircraft (HH-65C)	\$8,800,000.00	1	\$8,800,000.00	\$0.00	\$3,520,000.00
ship (SAFE Boats)	\$200,000.00	4	\$800,000.00	\$0.00	\$320,000.00
X-Band	\$1,000,000.00	1	\$1,000,000.00	\$0.00	\$300,000.00
X-Band(Suricate)	\$2,500,000.00	2		\$5,000,000.00	\$1,500,000.00
USV (Protector)	\$3,500,000.00	2		\$7,000,000.00	\$3,500,000.00
Thermo Sentry II	\$82,000.00	2		\$164,000.00	\$8,000.00
				\$12,164,000.00	\$9,148,000.00
				Total FY07 cost	\$21,312,000.00

Table 43. Total Cost for Alternative E

Current + USV + Two Additional Radars + Thermo Vision Sentry II + Thermo Vision Sentinel (F)

Table 44 summarizes the total cost for alternative F.

	Est. Procurement Cost	Quantity	Sunk Cost	Procurement Cost	O&S Cost
Manned aircraft (HH-65C)	\$8,800,000.00	1	\$8,800,000.00	\$0.00	\$3,520,000.00
ship (SAFE Boats)	\$200,000.00	4	\$800,000.00	\$0.00	\$320,000.00
X-Band	\$1,000,000.00	1	\$1,000,000.00	\$0.00	\$300,000.00
X-Band(Suricate)	\$2,500,000.00	2		\$5,000,000.00	\$1,500,000.00
USV (Protector)	\$3,500,000.00	2		\$7,000,000.00	\$3,500,000.00
Thermo Sentry II	\$82,000.00	2		\$72,000.00	\$16,000.00
Thermo Vision Sentinel	\$36,000.00	5		\$180,000.00	\$40,000.00
				\$12,252,000.00	\$9,196,000.00
				Total FY07 cost	\$21,448,000.00

Table 44. Total Cost for Alternative F

Current + USV + Two Additional Radars + Thermo Vision Sentry II + Thermo Vision Sentinel + Networked Sensors + Sonar (G)

Table 45 summarizes the total cost for alternative G.

	Est. Procurement Cost	Quantity	Sunk Cost	Procurement Cost	O&S Cost
Manned aircraft (HH-65C)	\$8,800,000.00	1	\$8,800,000.00	\$0.00	\$3,520,000.00
ship (SAFE Boats)	\$200,000.00	4	\$800,000.00	\$0.00	\$320,000.00
X-Band	\$1,000,000.00	1	\$1,000,000.00	\$0.00	\$300,000.00
X-Band(Suricate)	\$2,500,000.00	2		\$5,000,000.00	\$1,500,000.00
USV (protector)	\$3,500,000.00	2		\$7,000,000.00	\$3,500,000.00
Thermo Sentry II	\$82,000.00	2		\$72,000.00	\$16,000.00
Thermo Vision Sentinel	\$36,000.00	5		\$180,000.00	\$40,000.00
Network Sensor array	\$2,500,000.00	2		\$5,000,000.00	\$1,000,000.00
Active Omni-directional	\$2,000,000.00	5		\$10,000,000.00	\$2,000,000.00
HF Tactical Sonar	\$1,500,000.00	4		\$6,000,000.00	\$1,200,000.00
				\$33,252,000.00	\$13,396,000.00
				Total FY07 cost	\$46,648,000.00

Table 45. Total Cost for Alternative G

6. Cost Benefit Analysis

As the number of sensors that are incorporated into the different sensor configurations increases, so does the cost of the configurations. Graphing the detection percentage compared to the cost is depicted in Figures 92 and 93. Each line segment is a particular number of terrorist threats and each point on each line segment represents the alternatives A-G respectively.

For example, if the desire of the stakeholder is to prevent three terrorist small boat attacks from reaching the Port of Oakland, he would need to determine the line with the appropriate characteristics from either of the graphs below. From the three terrorist line (yellow line in Figure 92), he would profile trace the path to the determined detection percentage the stakeholder desires. If the desired detection percentage is within the bounds of the three terrorist's line, he would proceed to the closest point along the line to determine the appropriate sensor package. The point to the far left on the point is A, the second point in same line is alternative B, etc. At that point, a desired cost of the configuration can be obtained.

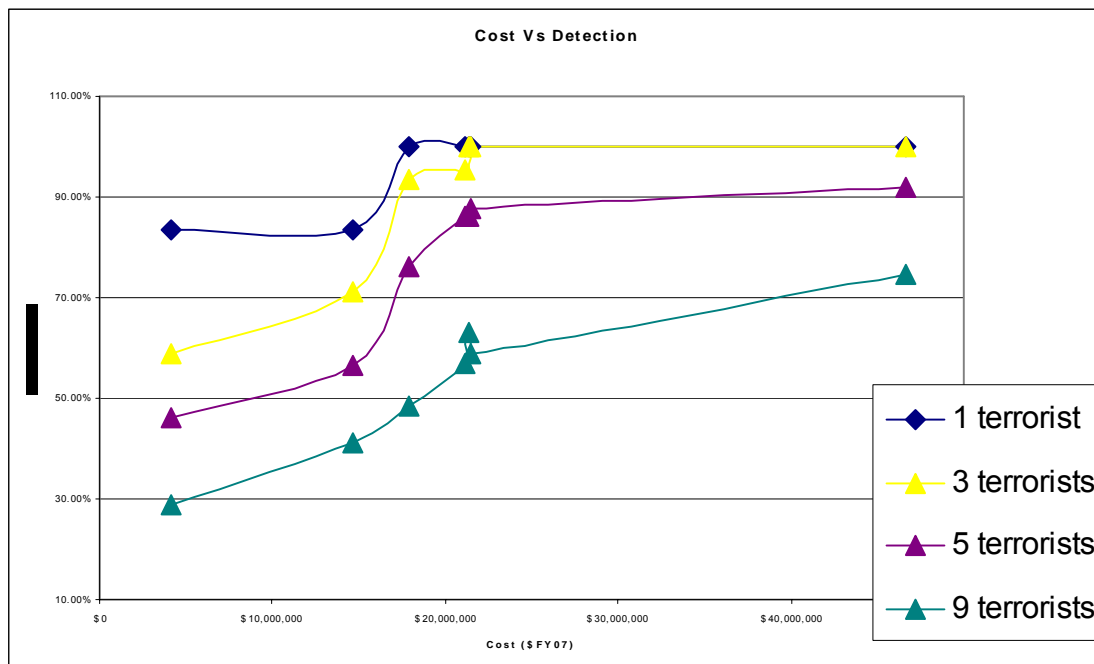


Figure 92. Cost vs Detection for Alternatives A-G with Odd Number Terrorists

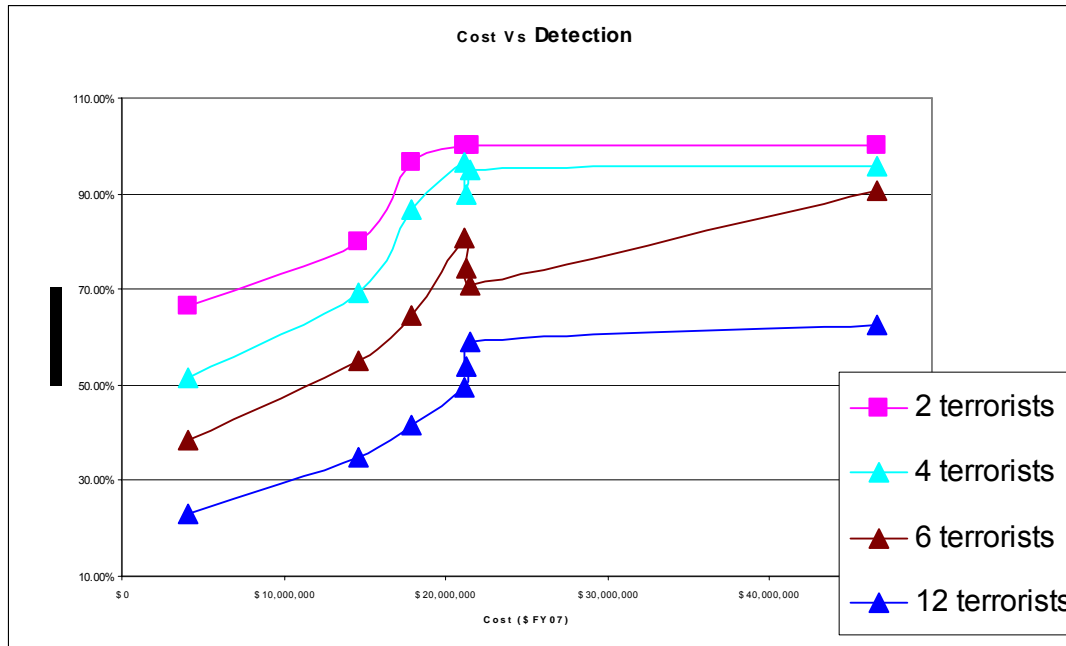


Figure 93. Cost vs Detection for Alternatives A-G with Even Number Terrorists

What the RSTG discovered was that for each number of terrorist threats, the most optimal configuration ranged. As with the optimal sensor configuration, the aspect of cost and detection percentages are huge driving considerations as well and can ultimately sway the stakeholder's consideration. Depending on the needs of the stakeholder which desire a particular sensor configuration, the final say rests in the hands of the stakeholder and therefore RSTG could only present the information.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. SOURCE SEABORNE THREATS GROUP

A. PROBLEM DEFINITION

1. Needs Analysis

a. *System Decomposition*

The system decomposition is a step during the needs analysis process that is used to identify what the current system addresses which enables the generation of possible solutions. Figure 94 presents the system decomposition for the SSTG. The system is decomposed into the components, functions, states and structure. They are intended to provide a framework to analyze the current system, elements, subsystems and components, and their relationships.

<u>Components</u> -Structural Source port, Sensors, Weapons, Communications Networks -Operational Personnel, Trucks, Ships -Flow C4I, Cargo/Passengers, Intelligence
<u>Functions</u> -Deny container holding undesired cargoes from loading onto container ship -Deny terrorist would-be crews onboard container ship -Detect and disrupt UAV attacks on container ship in-transit -Secure choke point leading to the domestic ports
<u>States</u> -In source port -Restricted movement transit -Open water transit
<u>Structure</u> -Internal to ship -Local -National -Regional Littoral States

Figure 94. SSTG System Decomposition

The components section is divided into structural, operational, and flow requirements needed for port security from the source port and in-transit aspect. The port

and its infrastructure, sensors, weapons and communication networks form the framework of the system. Personnel, trucks, and ships, are the integral components of the operational construct of the system in providing port security. The C4I (command, control, communications, computers, and intelligence) and the cargo are the elements that flow through the system.

The systems' functions are selected to address threats at the source port and transiting ships. At the source port, the system should deny containers enclosing undesired cargo from loading onto container ships. It should deny potential terrorists from boarding the ship as crew or passengers. The objective of these two functions is to curtail terrorist preparation activities at the source port. The system should also detect and disrupt UAVs attacking the transiting container ships.

These states describe different modes in which the system must operate. The ship may be located inside the port, in congested and restrictive waterways, or in open water during transoceanic transit.

The structure describes the command and control of the system and the interaction among personnel to assure the availability of security measures. The crew of the ship must coordinate with the port facilities, maritime authorities, security agencies, and law enforcement agents from the source port, transshipment ports, and the receiving port to ensure security from the source to the destination. This must be a coordinated effort including the governments of the littoral states whose waters the ship traverses.

b. Stakeholder Analysis

All stakeholders belong to at least one of four categories: clients, users, analysts, and others. The clients are the personnel, businesses, or agencies that make the decisions to allocate resources for the purchase, maintenance, and operation of the system. The users are the businesses and their personnel who are employed to operate the system. The analysts are businesses, agencies, and governments that have a vested interest in the analysis of the operation, success or failure of the system, and future viability. The others category relates to individual, business, agencies, and governments

that have an indirect vested interest in the success or failure of the system. Figure 95 presents the stakeholders considered the most essential to the security.

Clients:

- DOD
- Department of Homeland Security (DHS)
- Shipping Companies
- Domestic and Foreign federal, state, and local governments
- Port Owners
- Shipyard Owners

Users:

- United States Coast Guard
- USN
- Naval Station Command
- Foreign and Domestic Port Operators
- Foreign and Domestic Shipyard Operators
- Ship's Crew members

Analysts:

- DOD
- Department of Homeland Security (DHS)
- USN
- Commercial Security Consultants
- International Maritime Organization

Others:

- United Nations
- Shipping Merchants
- Consumers

Figure 95. SSTG Stakeholders

The stakeholders list was determined through an evaluative process resulting in site visits, phone interviews, e-mails, and video teleconferences with prospective clients, users, and analysts. Clients included foreign and domestic governments and port owners who determined that preventing undesired goods from entering the port area by land and sea was critical in providing port security for the source and destination ports. Identification of undesired cargo transiting unchecked to the destination port and being traced to the source port could have serious political ramifications for the originating port and the government in which the originating port is located. The source port would suffer enormous economic repercussions if WMDs were allowed passage to foreign territory. More specifically, all security agencies and practices at that port would be questioned and current trading practices would change.

A critical area the users identified in source port security is the lack of awareness and accountability in the hiring and background checks of personnel that operate and work on ships that frequent the ports. Additionally, a large portion of

shipping is done via transshipment in which the containers and crew are rarely screened as they are unloaded and reloaded from ship to ship. Although there are locking mechanisms on the containers, there are currently no additional measures in place to ensure that these containers are not tampered with in the process.

There is also the need to assess the economic impact on the operation of the source port from initial system layout and the economic burden of reduced throughput of containers and ships.

c. Input-Output Model

The input-output Model identifies the critical input parameters required for the system to operate and the desired and undesired outputs of the system.

The input-output model is displayed in Figure 96. The inputs and outputs are identified by examining the four primary functions the system needs to accomplish in order to address the needs at the source port and shipping in-transit. The four primary functions are:

- Deny container holding undesired cargo from loading onto container ship
- Deny terrorist crews access to the container ship
- Detect and disrupt UAV attacks on the transiting container ship
- Secure choke point routes to the domestic ports.

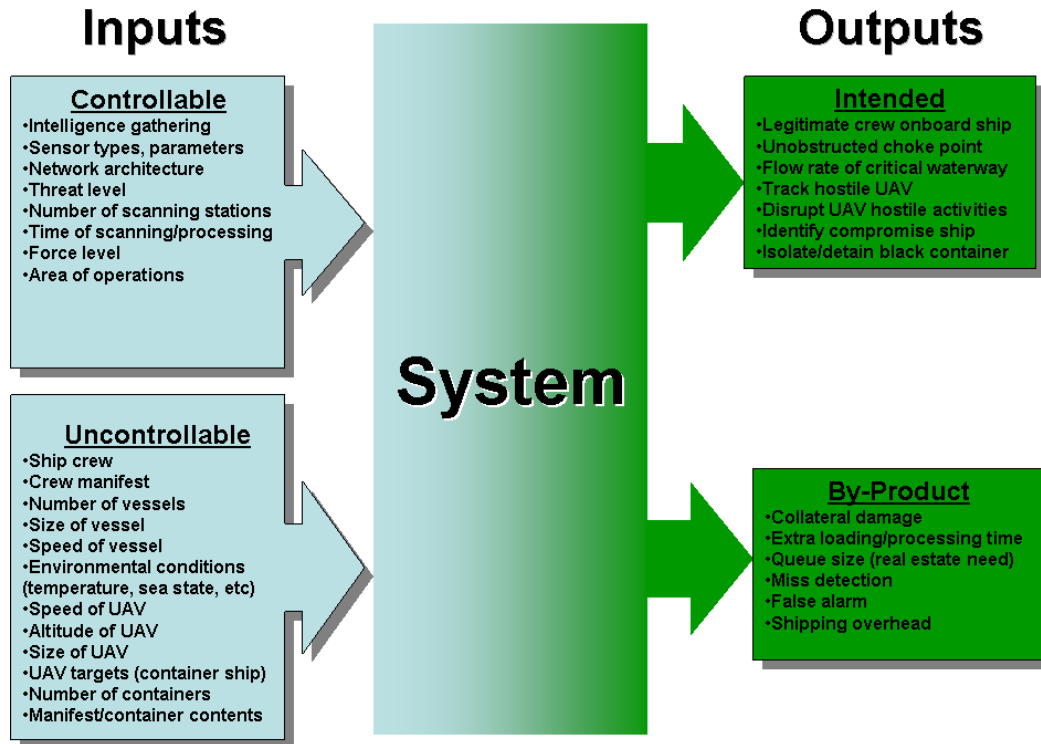


Figure 96. SSTG Input-Output Model

In Figure 96, under the controllable inputs, various types of sensors and the associated performance parameters, such as the transmission signal and the architecture of the sensor system, would affect the overall system performance. Other controllable factors that could also affect the system performance are the selection of the appropriate threat level and its associated measures, the number of scanning stations, the technology used for the scanning, the area of operations, and the amount of personnel needed to maintain the required operational effectiveness.

Uncontrollable inputs are those who cannot be totally manipulated by the stakeholder. The amount of relevant intelligence collected directly influences the mission success of the system. The type of targets and their associated operational profiles and specifications also affect the system's mission success. Environmental conditions, such as the temperature and sea state, also influence the system output.

Each of the four primary functions aims to achieve a desirable output from the system. At the source port, before the container ship leaves for the destination port,

only the legitimate crews should be authorized onboard the vessel. Prior to the loading of containers onto the ship, any container that is indeed carrying undesired cargo must be quarantined and inspected. During the transit, any hostile UAV attempting to deploy WMD onto the ship's hull, containers, or deck should be detected, tracked, and disrupted. In the vicinity of the destination port, where natural and manmade chokepoints are present at the port of entry, the ideal state is to maintain an unobstructed traffic flow in the essential water route.

There are additional by-products that are undesirable that the system requires minimizing the impact. By-products of a system include:

- Collateral Damage
- Extra loading and processing time
- Real estate needs to manage queue size
- Miss detection
- False alarm
- Shipping and cost overhead

d. Functional Analysis

Figure 97 is the functional flow diagram to deny containers holding undesired cargo from loading onto container ships. The sub-functions are to screen the container's manifest, conduct either a non-intrusive or intrusive inspection, or both. For countries considered to have hazardous cargo, either quarantine or load the flagged containers depending on what is found by investigation to determine if the cargo is legitimate.

The CBP requires the shipper to complete manifests and bills of lading information. This information is to be submitted to the CBP 24 hours in advance of the cargo being loaded onto the container ship at foreign ports [14]. These manifests are then screened to identify containers that contain potentially dangerous cargo. Screening attempts to identify possible anomalies that suggest the actual contents do not match the description of the manifest. Containers that do not pass the manifest screening are segregated for higher level inspections. The subsequent inspection is composed of non-intrusive and intrusive methods. Non-intrusive scanning is performed using external sensing devices or human senses to scan the container for suspicious sensory signatures

without opening the container and examining every single item inside. This type of scanning also includes weighing the container to confirm the weight of stated cargo is within an acceptable confidence level for the goods stated in the manifest. The objective of the scanning is to detect weight anomalies as well as traces of chemical, biological, radiological, and explosive substances emitted from the containers. A useful by-product of this function is the detection of contraband items. Intrusive inspection requires removing the items from the container for thorough inspection. A failed non-intrusive scanning is typically followed by an intrusive inspection.

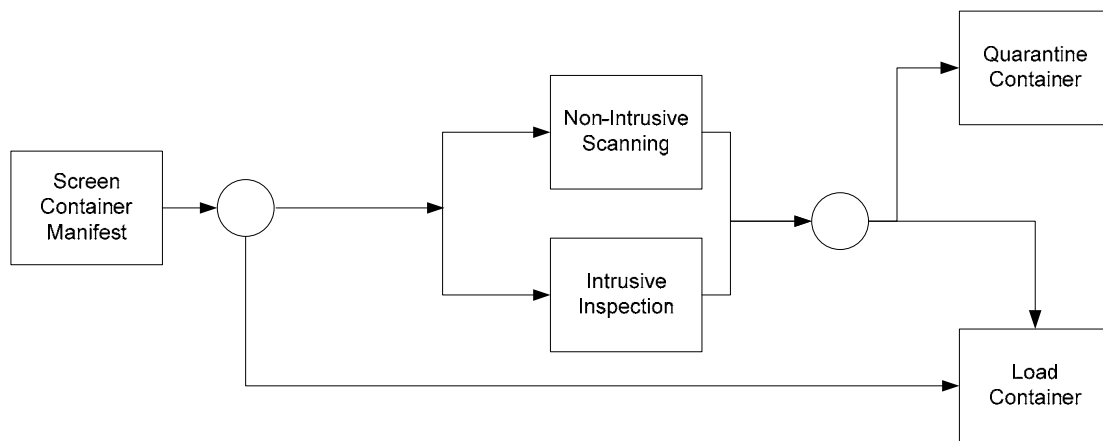


Figure 97. Deny Loading of Undesired Cargo Functional Flow Diagram

Containers that have passed the preliminary manifest screening or follow-up inspection would proceed to be loaded onto the container ship, or placed in a storage area while waiting the arrival of the container ship. Containers carrying items that fit the description of the undesired cargo would be quarantined and inspected. The focus of this study is to detect containers carrying undesired cargo prior to the loading onto container ships.

Figure 98 is the functional flow diagram to deny terrorist access to the container ship. The system shall gather intelligence data from the network of databases to collate and identify container ships, captains, and sailors that have access to the port facilities and the ship. The identification process may determine that an individual or group of people could pose a security threat to the port or ship. A ship that has been

identified as having one crew member who could be a security threat to the port would be denied port entry.

The ship's entry could be denied by securing the port or most likely interdicting the ship in open waters by the appropriate agency. If the ship has already berthed at the dock or has managed to gain access to the port, all of the ship's crew would be denied access to the port facility. The appropriate agencies would be notified to investigate and detain the suspected individuals. The final stage of the functional flow is to neutralize the threat. Once the ship's crew members have been denied entry to the port facilities, the threat has to be neutralized. The neutralization process would include the notification of appropriate local, state, and national government agencies to detain and prosecute the suspected crew member(s).

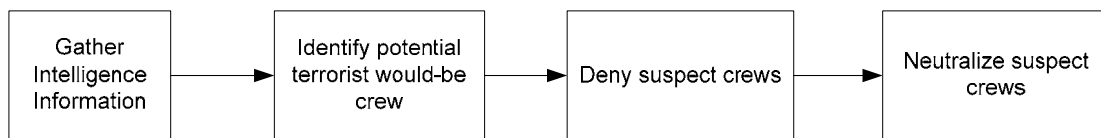


Figure 98. Ship's Crew Infiltration Functional Flow

The functional flow diagram to detect and disrupt UAV attacks on a container ship is shown in Figure 99.

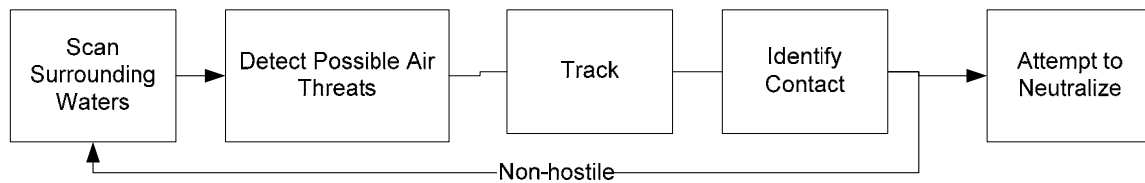


Figure 99. Detect and Disrupt UAV Attack on Transiting Ship Functional Flow

A ship employing this system would need to maintain awareness by scanning the surrounding area. Air surveillance radars would be used to create an image of the area surrounding the ship, enhancing situational awareness. All contacts would be tracked. Based on the contacts behavior (such as speed, altitude, and direction), the target would be identified as either hostile or neutral. An identified hostile contact could be

neutralized by non-lethal means. An example of neutralization is the use of audio warnings to delay the attack, which provides the container ship time to seek further assistance from other entities. This process is constantly iterative, occurring the entire time that the vessel conducting the search while transiting in high risk regions. The high seas regions were not considered as there is low probability of occurrence due to the required range which is currently unachievable by the terrorists.

Figure 100 is the functional flow diagram to secure navigation-restricted water routes to the ports. The sub-functions are as follows:

- Collect PANS in advance of vessel approach to chokepoint and strategic waterway
- Scan for dangerous cargo at source ports
- Monitor vessel traffic near and within strategic waterway and chokepoint
- Obtain hostile ship information from intelligence
- Analyze & identify targets & threats
- Monitor probable threats
- Escort probable threats
- Handover probable threat to respective agency

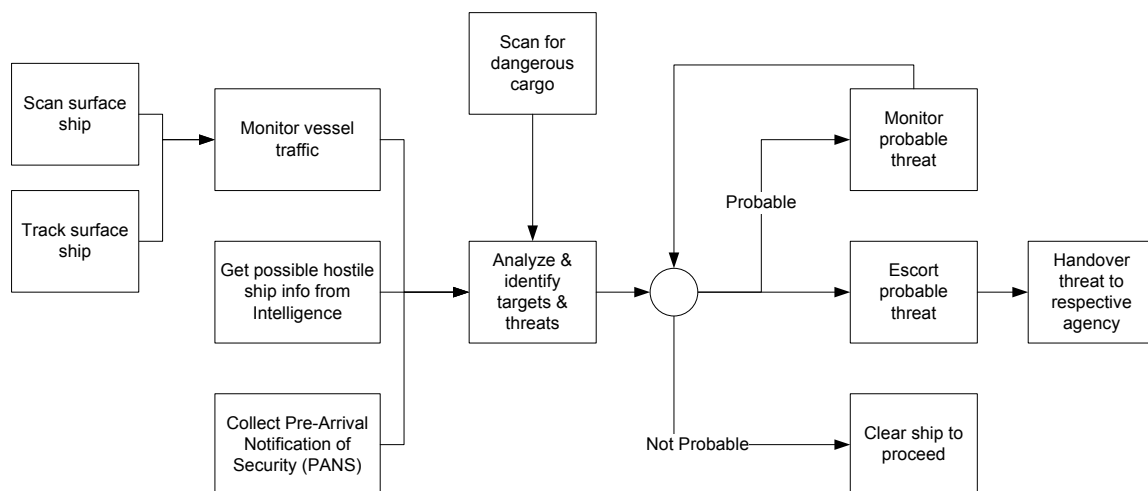


Figure 100. Secure Chokepoint Loading to Port Functional Flow

Prior to the vessel's arrival at the strategic waterway, initiatives to ensure its security include scanning for dangerous cargo and submission of PANS documents. At the strategic waterway and chokepoint, the system should monitor vessel traffic transiting into and within the vicinity. Through scanning and tracking surface vessels, the

system searches for suspicious activity that warrants additional investigation. High traffic density around the vicinity of high-value targets poses challenges to the system in identifying suspicious activity. Intelligence would be a vital input element in the threat and targeting analysis. Intelligence enables the system to perform threat analysis and generate a potential threats list. Resources would be recommended for deployment to protect high-value assets.

The output of the threat and targeting analysis delivers the likelihood of each vessel posing a threat to the waterway and other vessels. The maritime security authority handles threats according to their risk factors. If the threat probability is deemed low, the vessel would be cleared to proceed through the strategic waterway. If the threat probability is deemed moderate, the threat would be monitored closely and provided with an escort if necessary. For cases when the threat is very likely, the maritime security authority and other local agencies might deny the vessel transit through the chokepoint. The focus of this study is to detect and prevent threatening vessels from inflicting damage near or within a strategic waterway.

2. Objectives Hierarchy

The objective hierarchy provides the means to evaluate the concerns of the system and the lower tier of the evaluation measures are adequately measure to attain the system objective. The MOEs and MOPs are the quantitative measures used to evaluate the different alternatives generated for the system design. During the modeling and analysis phase, the MOEs and MOPs serve as a guide to design the models in order to analyze the various alternatives. Figure 101 depicts the objectives for “deny container holding undesired cargo from loading onto container ship,” while Table 46 describes the associated MOEs and MOPs for the function.

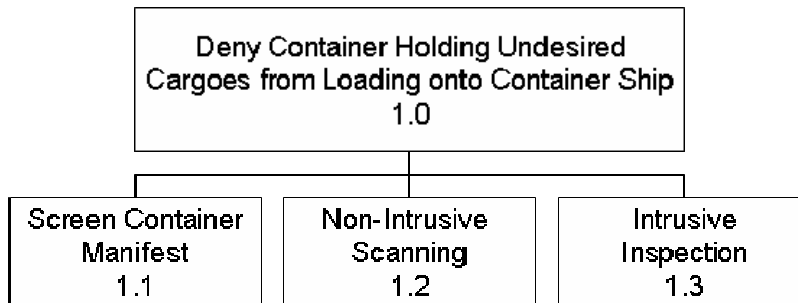


Figure 101. Objectives Hierarchy for Deny Container Holding Undesired Cargo

MOEs/MOPs		Objective Item
MOE :	Accuracy of Manifest Screening	Screen Container Manifest – 1.1
	MOP: Probability of Detecting Anomalies	
	MOP: Probability of Type I Error	
	MOP: Probability of Type II Error	
MOE:	Timeliness of Manifest Screening	Screen Container Manifest – 1.1
	MOP: Average Time to Process Manifest	
	MOP: Average Number of Manifests Processed per Day	
MOE:	Accuracy of Scanning	Non-Intrusive Scanning - 1.2
	MOP: Probability of Detecting Undesired Cargo	
	MOP: Probability of Type I Error	
	MOP: Probability of Type II Error	
MOE:	Timeliness of Scanning	Non-Intrusive Scanning - 1.2
	MOP: Average Scan Time Per Container	
	MOP: Number of Containers Scanned Per Day/Hour	
MOE:	Accuracy of Inspection	Intrusive Inspection - 1.3
	MOP: Probability of Verifying Undesired Cargo	
	MOP: Probability of Type I Error	
	MOP: Probability of Type II Error	
MOE:	Timeliness of Inspection	Intrusive Inspection - 1.3
	MOP: Average Inspection Time per Container	
	MOP: Number of Containers Inspected Per Day/Hour	

Table 46. MOE/MOP for Deny Container Holding Undesired Cargo from Loading

Figure 102 depicts the objectives for “detect and disrupt UAV attack on a container ship in-transit,” while Table 47 describes the associated MOEs and MOPs for the function. In the UAV attack scenario, there will be little time after an air vehicle is detected to consult other intelligence agencies or to summon local area enforcement for assistance. The SSTG is focusing on the pre-attack aspect and leaving the response methods as a topic for further study.

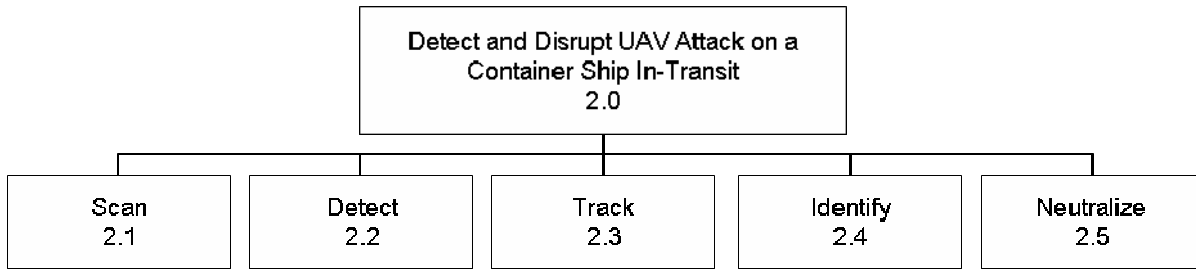


Figure 102. Objectives Hierarchy for Detect and Disrupt UAV Attack

MOEs/MOPs			Objective Item
MOE :	Coverage		Scan - 2.1
	MOP:	Range	
	MOP:	Azimuth	
	MOP:	Elevation	
MOE:	Frequency		Scan - 2.1
	MOP:	Scan Rate	
MOE:	Detection Quality		Detect - 2.2
	MOP:	Resolution	
	MOP:	Probability of Detecting UAV	
	MOP:	Probability of Type I Error	
	MOP:	Probability of Type II Error	
MOE:	Information Availability		Detect - 2.2
	MOP:	Speed of UAV	
	MOP:	Direction of UAV	
	MOP:	Altitude of UAV	
MOE:	Timeliness		Track - 2.3
	MOP:	Revisit Time	
MOE:	Track Quality		Track - 2.3
	MOP:	Probability of Maintaining Track	
	MOP:	Probability of Lost Track	
MOE:	Multiple Contact Capabilities		Track - 2.3
	MOP:	Maximum Number of Contacts Tracked	
MOE:	Identification Accuracy		Identify - 2.4
	MOP:	Probability of Correct Identification	
	MOP:	Probability of Type I Error	
	MOP:	Probability of Type II Error	
MOE:	Neutralization Effectiveness		Neutralize - 2.5
	MOP:	Percent of Threats Neutralized	
	MOP:	Minimum Effective Range	
MOE:	Suitability		Neutralize - 2.5
	MOP:	Average Time Required to Deploy	

Table 47. MOE/MOP for Detect and Disrupt UAV Attack on Transiting Container Ship

Figure 103 depicts the objectives for “deny terrorist access onboard container ship,” while Table 48 describes the associated MOEs and MOPs for the function.

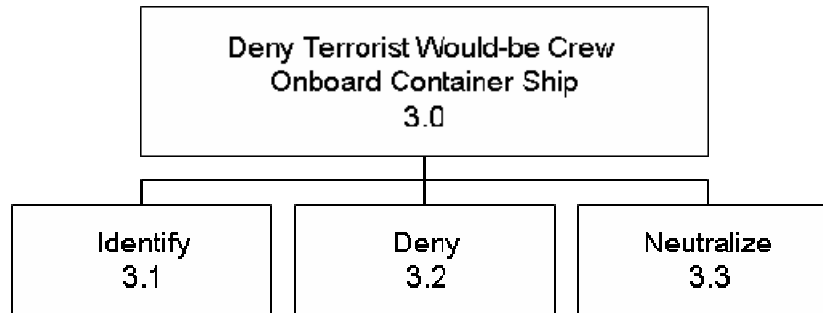


Figure 103. Objectives Hierarchy for Deny Terrorist Access Onboard Container Ship

MOEs/MOPs			Objective Item
MOE :	Intelligence Data Handling Capability		Identify - 3.1
	MOP:	Probability of Correct Identification	
	MOP:	Average Time to Identify a Threat	
	MOP:	Probability of Type I Error	
	MOP:	Probability of Type II Error	
MOE:	Timeliness		Deny - 3.2
	MOP:	Average Time to Notify Appropriate Agencies	
	MOP:	Probability of Type I Error for Denial	
	MOP:	Probability of Type II Error for Denial	
	MOP:	Average Response Time to Locate and Detain Identified Crew Members	
	MOP:	Average Time Required to Process Identification of Suspect Crew Members	Neutralize - 3.3
MOE:	Effectiveness		
	MOP:	Average Time of Port Operations Disruptions due to Threat Neutralization	
	MOP:	Percentage of Equipment Downtime during Neutralization	
	MOP:	Manpower Required to Neutralize Typical Threat	

Table 48. MOE/MOP for Deny Terrorist Access Onboard Container Ship

Figure 104 depicts the objectives for “secure chokepoint leading to the domestic ports,” while Table 49 describes the associated MOEs and MOPs for the function.

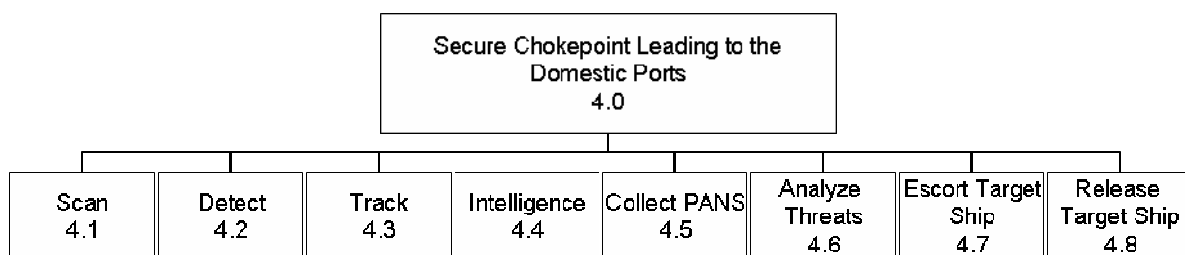


Figure 104. Objectives Hierarchy for Secure Chokepoint Leading to Domestic Port

MOEs/MOPs			Objective Item
MOE :	Target Search		Scan - 4.1
	MOP:	Search Rate	
MOE:	Target Acquisition		Scan - 4.1
	MOP:	Proportion of Acquisitions vs Detections	
	MOP:	Average Acquisition Range	
MOE:	Coverage		Scan - 4.1
	MOP:	Range	
	MOP:	Azimuth	
	MOP:	Elevation	
MOE:	Frequency		Scan - 4.1
	MOP:	Scan Rate	
MOE:	Detection Quality		Detect - 4.2
	MOP:	Resolution of Measurements (e.g. speed, direction)	
	MOP:	Probability of Detection	
	MOP:	Probability of Type I Error	
	MOP:	Probability of Type II Error	
MOE:	Information Availability		Detect - 4.2
	MOP:	Speed	
	MOP:	Direction	
MOE:	Timeliness		Track - 4.3
	MOP:	Revisit Time	
MOE:	Track Quality		Track - 4.3
	MOP:	Probability of Maintaining Track	
	MOP:	Probability of Losing Track	
	MOP:	False Track Rate	
MOE:	Multiple Contact Capabilities		Track - 4.3
	MOP:	Maximum Number of Tracks at Once	
MOE:	Timeliness		Intelligence - 4.4
	MOP:	Time that Intelligence is Obtained and Measured with respect to Hostile Ship Leaving Port	
	MOP:	Time that Intelligence is Obtained and Measured with respect to Hostile Ship Entering Port	
MOE:	Accuracy of Source		Intelligence - 4.4
	MOP:	Probability of Intelligence Showing a Real Threat	
MOE:	Credibility of Source		Intelligence - 4.4
	MOP:	Credibility Rating of Source	
MOE:	Coincidence		Intelligence - 4.4
	MOP:	Number of Sources with Coinciding Information	
MOE:	Timeliness		Collect PANS - 4.5
	MOP:	Time in Advance that PANS is received	
MOE:	Detail of PANS Document		Collect PANS - 4.5
	MOP:	Relevance of Questions	
	MOP:	Depth of Questions	
MOE:	Authentication of Informer		Collect PANS - 4.5
	MOP:	Trustworthiness of Informer	
	MOP:	Availability of Source Port Counter-Checking PANS with Ships Document	
MOE:	Quality of Analysis		Analyze Threats - 4.6
	MOP:	Minimum Amount of Information Needed to Run Analysis	
	MOP:	Uncertainty in Analysis Results	
	MOP:	Ability of Analysis to Incorporate and Infer from Up-to-Date Real World Incidents	
MOE:	Performance of Analysis		Analyze Threats - 4.6
	MOP:	Probability of Correctly Identifying Threats	
	MOP:	Proportion of Valid Predictions of the Situation	
	MOP:	Proportion of Correct Forecasts	
	MOP:	Proportion of Estimates Containing Complete Predictions	
	MOP:	Spread of Analysis Results (how many ships are probable?)	
MOE:	Suppression Ability		Escort Target Ship - 4.7
	MOP:	Firepower to Deter Potential Wrongdoers	
	MOP:	Firepower to Neutralize Wrongdoers	
MOE:	Speed of Operations		Escort Target Ship - 4.7
	MOP:	Average Time from Decision to Issuing Requests or Reports	
	MOP:	Response Time of Escort	
MOE:	Speed of Operations		Release Target Ship - 4.8
	MOP:	Average Time to Disseminate Orders	

Table 49. MOE/MOP for Secure Chokepoint Leading to Domestic Port

B. DESIGN AND ANALYSIS

1. Alternatives Generation

The Maritime Transportation Security Act (MTSA), signed into law by President George Bush in November 2002, has some far reaching implications for the development of robust designs that allows for accurate and efficient scanning of undesired cargo. Cargo inbound to the U.S. from foreign source ports on container ships may be denied entry into U.S. territorial waters by the DHS if the source ports are found to be consistently lacking in adequate security and screening of cargo [46]. The source port group is not limiting a source port to be identified as a port that only has inbound cargo to the United States, but rather any port that exports containerized cargo to another country. The implications of the MTSA on the world's view of port security measures could have ripple effects to other countries that may also deny inbound cargo from suspect ports that do not provide adequate cargo screening.

The SSTG developed alternatives based on the premise that a source port would be receiving container cargo from land routes (trucks carrying containerized cargo) and through transshipment (containerized cargo that is off-loaded from one ship to another ship in the port). During the initial alternative generation, all methods were considered regardless of cost or impact on port operations. A morphological chart and feasibility screening were used to narrow the generated alternatives to a realistic number that was bound by the constraints of available technology by 2012, stakeholder inputs, and minimal impact on port operations, in particular container throughput.

a. Considerations for Alternatives

Installation of Scanner

The installation of scanning equipment was considered for subsequent modeling and analyzing the overall system effectiveness. The mobile system is generally installed in a van or truck that can freely travel within the port to scan containers and shipping trucks. The mobile unit brings the scanning equipment to the targeted containers for non-intrusive scanning. The mobile system is equipped with digital

imagers that automatically highlight any suspicious cargo and can be utilized to scan the entire container or certain areas.

Scanning systems located on the crane already exist as weight scales. The scales are effective in determining if the container matches the cargo weight stated in the cargo manifest. The incorporation of X-ray and neutron imagers onto the crane loaders is being developed and will be available by 2012. Each container would be scanned and imaged while being lifted by the crane loader. The combining of lifting and scanning concurrently enables the port operator to execute 100 percent volume scan of all containers. Currently, information is not available on the performance of the crane loading scanners and if such technology requires extra time to lift each container due to the scanning requirement. Although Port of Oakland has conducted the trial using crane loading scanners, the results have not been released.

Fixed entry point scanning is already implemented in Singapore and other ports. Every container truck must pass through a scanning system at the entry point of the port, making 100 percent volume scanning for all containers possible. Utilizing the newest X-ray and gamma ray imagers, the trucks can be scanned as they traverse through the entry in approximately eight seconds. However, transshipment containers arriving from the waterside will have to be scanned using the mobile system or the crane loading scanner.

Intrusive Inspection

Intrusive inspection seeks to verify suspicions of container cargo following an initial stage of screening. The initial stage of screening includes manifest screening and non-intrusive inspection of the container among other procedures that could lead port authorities to doubt the integrity of the container cargo.

When a container is flagged for intrusive inspection, its origin or its contents are suspected and the key objective of intrusive inspection is to accurately identify and locate any suspected cargo within the container. If the call to inspect the container is a false alarm, then the process of intrusive inspection has to be precise and

prompt. Both requirements are important to ensure that suspected cargo is cleared or confirmed at a rate that causes minimum disruption to port operations.

The key elements of intrusive inspection are human inspectors, assisted with trained animals, portable radiation detectors and potentially remotely-controlled robot inspectors.

Given the sheer volume of cargo within a container and the potential danger involved, human inspectors are not expected to do a carpet search of all cargo or physically handle the suspected cargo. The value of human inspectors lies within their ability to integrate their understanding of the entire situation (manifest screening, non-intrusive scan results, anomalies in the real world) to better direct search efforts and harness the appropriate technology to conclude the search accurately and promptly. During a container search, trained animals are guided to search within the container and deploy portable radiation detectors and identifiers in the more probable regions.

Animals can be also trained to aid port security on different dimensions. Trained sea lions and dolphins are able to locate underwater divers. Trained dogs can be employed to detect drugs, bombs and now DVDs. Their olfactory ability is sensitive enough to detect trace amounts of many compounds, which makes them very effective in screening objects, in particular to detect drugs, humans and explosives. Dogs require close proximity to the cargo being searched and can take a considerable amount of time to screen a container. In addition, dogs require constant training to remain proficient and alert to detect a particular search item.

Today's security challenges are complicated. Commercial businesses ship radioactive material with valid commercial purposes. Terrorists may ship radioactive material in their bid to build WMDs. The human inspector requires equipment such as a portable radiation inspectors to instantly reveal the precise nature of radioactive contents. The portable radiation inspector needs to be sensitive and accurate in identifying the type of radiation present in the suspected container. Its job is complicated by the natural cosmic radiation all around us, unintentional radiation from manmade materials (e.g. ceramic tiles) and the intentional shielding of any radioactive material that is being

smuggled. The portable radiation inspector needs to inform the inspector of the precise radioactive contents in order to conclude the search. The portable radiation inspector is required to maintain a low false alarm rate and to minimize disruptions to port operations and public confidence. Various national laboratories in the U.S. have been focusing on radiation detectors. They include Sandia National Laboratories, Radiation Detection Center at Lawrence Livermore National Laboratory, and Oak Ridge National Laboratory.

The previously-mentioned national laboratories have been focusing on radiation detection portals and portable radiation devices. Given the dangerous nature of cargo inspection to the human inspector and trained animals, it is not unreasonable to forecast the use of robotics to take over this job. However, tremendous technical challenges in radiation detection and in robotic automation have to be overcome before such robot inspectors are technically and commercially viable to incorporate into cargo search.

Manifest Screening

The manifest screening aspect of the container security process describes the use of information about the containers and cargo that does not originate from the scanning process. The system uses the information to determine the container's threat level and to organize the scan and search operations. Without manifest screening, port operators would not have any advanced notice about the type of cargo arriving at the port. The selection of container for scanning would be random at the source port. All intelligence regarding the containerized goods would be collected from non-intrusive and intrusive searches conducted in the source port.

ATS (Status Quo)

Currently, the CBP in coalition with the USCG have two enforced rules for cargo reporting that are destined for U.S. ports.

On 2 December 2002, the 24 hour cargo manifest rule was enforced. This rule requires carriers to submit a declaration to CBP 24 hours prior to cargo loading in a foreign port. The CBP enters this data into the Automated Targeting System (ATS) that is linked to various commercial and law enforcement agencies. The ATS uses the

information to search for pattern anomalies and cargo of interest. The ATS system was created after 9/11 from a similar system that CBP was in use. The Automated Manifest System (AMS) stored information about the participants in the shipping industry and their shipping patterns. ATS provides a more thorough search, and generates a numerical score for each container. Higher scores equate to higher risks. This law was in full enforcement by 2 May 2003. Fines were being issued to the shipper who had filed incorrect information and “Do Not Load” messages were being sent to port operators for the containers that were not properly documented.

The USCG also requires all commercial vessels, foreign or domestic, entering a U.S. port from a foreign port to give a 96 hour advance notice of arrival. A cargo manifest must be electronically submitted to the National Vessel Movement Center (NVMC) for screening. The NVMC is linked to other agencies and databases to detect suspicious cargo and to alert the USCG before the ship’s arrival in port.

ATS+

In the ATS (status quo), only the shippers are required to submit manifests to CBP. The shippers usually get the necessary data from the exporter to complete the manifest and there is no requirement for the exporter to submit the manifest. The level of inspection conducted by the shipping company prior to loading the container will depend on several factors. Usually, shipping companies will accept reports from trusted exporters as truth and transfer the reports to CBP. This process presents a gap for the exporter to exploit permitting an opportunity to smuggle undesired cargo into the United States. A ship operated by a rogue crew could easily forge the manifest by adding the number of containers shipped from a particular exporter and their own containers packed with explosives and radiological material without causing suspicion.

However, if manifests are required separately from the exporter, shipper and importer, a more complete image can be generated on the item being shipped. Discrepancies would be easily flagged when the three submissions are collated for consistency. A terrorist cell would have to infiltrate or create their own exporting, shipping, and importing company, and coordinate the manifest filings for each in order to

smuggle undesired cargo. In ATS (status quo), either the shipper or the exporter would have to be infiltrated in order to transport undesired cargo to a U.S. port.

Data Sharing

Data sharing among the authorities and agencies would enhance the awareness of the global containers shipment. There are two forms of data sharing described as separate alternatives below. Additionally, data sharing also includes sharing intelligence gathered via intelligence agencies and as manifests and information collected via the non-intrusive scanning and intrusive searching. The goal of the data sharing is to streamline the intelligence gathered together with the scanning and search results into one cohesive report that is readily accessible by the correct authorities at the right time. This method would allow for further inspection of scan results while the ship is in-transit if the need arises. The USCG could decide if the ship should be stopped and searched at sea or allow the ship to enter the destination port. Without data sharing, the results of the non-intrusive scan would remain with the source port.

b. Status Quo Alternative

The Status Quo alternative describes the container security being practiced at the U.S. domestic ports. Containerized cargo arriving at the port facility via trucks would be screened for undesired materials. Transshipment containers, which constitute the major portion of the port's shipping container volume, are excluded from the screening process due to sheer lack of resources and additional overhead cost.

The ATS developed by the CBP is adopted to analyze shipping manifests (bill of lading and information) and customs documents to profile containers on risk of carrying undesired cargoes into the United States. Based on certain rules set, high-risk containers would be flagged as potential threats and of these potential threats, some are randomly selected for non-intrusive scanning before loading at the source port or at the port of entry in United States. Currently the ATS flags approximately six percent of all containers as potential threats [47].

At the source port, every container delivered by land vehicles is scanned at the point of entry into the port. The container will also be weighed to spot any anomalies by the experience operators. Radiation detectors will also be deployed to detect radioactive signatures.

Containers are also randomly selected for intrusive inspection. Intrusive inspection of containers is performed by human beings. Human inspectors would use portable radiation detectors to verify radiological materials. They will also be assisted by trained dogs to sniff for explosives.

c. Zero Percent Inspection Alternative

The zero percent volume screening alternative does not perform container scanning and inspection. It is proposed on the basis that current random screenings are not effective at meeting the performance of detecting unwanted cargo. In March 2006, the Government Accountability Office reported that there is no control to provide reasonable assurance that ATS is effective at targeting containers with the highest risk of smuggled weapons of mass destruction [48]. As such, this alternative does not perform any screening, scanning and inspection of containers.

d. 100 Percent Volume Screening Alternative

The 100 percent volume screening alternative is formulated upon the ambitious goal to scan each and every container that passes through the source port. This alternative applies the scanning approach to both incoming and transshipment containers. This is a huge increase in scanning requirements over the status quo of six percent of all containers identified by ATS for inspection.

In order to handle the huge volume of containers passing through each source port, this alternative incorporates a non-intrusive scan of each container at its essential waypoints in the port, namely at its point of entry into the port and while being lifted by the quay crane and yard crane. By incorporating scanning efforts in the essential waypoints, additional overhead to the current processing time could be minimized. The technologies used in this alternative are passive devices, such as weighing scales,

radiation detectors, and X-ray scanners. The (crane) operator experience and training proficiency would be a critical factor of the overall system performance. Figure 105 shows three potential radiation detectors that could be used in the port.



Figure 105: Handheld and Fixed Structure Radiation Detectors [49]

In current port operations, cranes fail to reach their specified productivity due to yard delays. For instance, the operator interference and proficiency in crane loading and machinery delays could introduce additional container processing time. Current state-of-the-art cranes, such as the Tandem 40s, are specified to load or unload a container in ideally 39 seconds which includes 30 seconds of crane mechanical movements and confirmation of pickup and deposit positions [50]. Yard delays prolong the turnaround time to 60 seconds. This provides a window of opportunity of duration of approximately 30 seconds to scan each container on the crane. Crane scanning technologies would have to meet this time requirement to minimize the economic cost of this alternative.

Containers that fail the scanning either at the point of entry or lifted by the crane are further screened using intrusive methods that is more thorough. Technologies used at this stage include human inspectors, trained animals and portable radiation detectors.

Given the comprehensive scanning efforts that have been invested into verifying each container, the source port will protect the integrity of the scanned container with smart tags that stores the cargo information and is hardened with tamper-proof lock. That information will be shared with destination ports authority to alleviate

their scanning requirements and for anomaly-checking in the event that the container has been tampered with.

Given that this alternative scans every container, there is no need to use ATS for targeting.

e. Improved Loading Inspection Alternative

The improved loading search alternative was based on improving the physical inspections that occur during the loading of containers. This method examines the concept that physical searches improve the detection of undesired goods more effectively than the use of intelligence. As part of the improved loading search alternative, ATS would remain as is by providing no information prior to container loading. Additionally, no data sharing mechanisms would be in place to exchange data regarding each container to the respective destination ports.

Non-intrusive screenings would occur during the loading process by positioning the sensors on crane spreaders. X-ray scanners, radiation detectors, and neutron scanners would provide scanned images of the containerized goods. Additionally, scales and operator experience would aid in detecting anomalies or unevenly distributed containers. Since the scanners would be on every crane, 100 percent of the containers loaded from trucks and containers loaded from another ship would be inspected.

Containers not passing the non-intrusive screening would immediately be removed from the loading area for an intrusive inspection. Humans, animals, and portable radiation detectors would be used to search for contraband. As no intelligence is being used to determine if a container needs an intrusive search, the decision would be based on the results from the non-intrusive search.

f. Minimum Port Operations Disruption Alternative

In contrast to the previous alternative, the minimum port operations disruption alternative relies on maximizing intelligence gathering in order to keep ship loading on schedule, preventing ships from being delayed while containerized goods are visually searched by humans.

An act is currently being supported in Congress that proposes the importer, exporter and the shipping company to submit cargo manifests to the CBP screening headquarters twenty-four hours before the containers are to be loaded at the source port. This system, known as ATS+, would provide a huge advantage over ATS (status quo) which only requires the shipping company to provide a manifest twenty-four hours prior to reaching its destination port. This information provides a much more complete picture of the shipping domain. Computers would rapidly distinguish containers with varying or vague manifests.

At the port, containers are scanned by the sensors mounted on the crane spreaders during transfer. The correlation of X-ray images, radiation signatures and gamma-ray energy levels would be used to calculate the probability of undesired cargo being present in the container. Operator experience would play a vital role in comparing items listed in the manifests with actual container weight, providing an additional layer of detecting container anomalies.

Those containers flagged as high risk through intelligence screening and fail the non-intrusive inspection would be transported to a temporary holding site located a safe distance from the port's critical infrastructure. The exporters are contacted to remove the containers sitting in the holding cell. The container can be resubmitted for shipment after the documentation and cargo issues are resolved. This plan provides a heavy economic impact for improper cargo and manifests submissions. It would provide a strong economic incentive for the exporter, importer and shipper to ensure that manifests are correctly documented and only legitimate cargo is packed inside the container.

Finally, the smart tags would be attached to provide container integrity throughout the shipment. Any tampering incident would trigger an instant notification to the subscribers of the container security network. Data from the screening process is also uploaded into the destination port so that the port authorities can further screen the information if deemed necessary.

g. High Performance Alternative

The high performance method uses the maximum capability of every aspect of the container screening process. This plan is probably the most expensive to implement, but provides a very interesting modeling alternative for comparison with the other alternatives. “Does the cost of the high performance alternative prove itself through much greater detection rates? Will the additional advanced screenings add cost to the operations without increasing the operating performance?” are questions that need to be answered.

The ATS+ provides thorough manifest processing to generate a list of containers of interest. ATS+ mandates that the exporter, the importer, and the shipper all provide manifests to the screening agency twenty-four hours prior to container loading. A mobile system as well as a sensor suite on the crane spreaders provides non-intrusive scanning capability. Each suite will include x-ray and gamma ray scanners accompanied by radiation detectors and neutron scanners. Scales and operator experience aids in anomaly detection. As 100 percent of the containers are non-intrusively inspected by this method, those requiring further inspection as a result of identification by the ATS+ or failing the non-intrusive scanning are removed and inspected by remotely-operated robots. Each robot would be operated by one human. The robot would prevent unnecessary risk for humans or animals entering the container to conduct inspections. Additionally, the robot is equipped with computers to process images and odiferous computation. The data collected by the robot will be searched within the library of threat signatures.

Smart tags would also be used to protect the containerized cargoes. Lastly, data from the screening is uploaded into the destination port to provide the officials in the destination port with a complete container history prior to arrival.

h. 100 Percent Intrusive Inspection Alternative

The 100 percent intrusive inspection concentrates the effort to inspect every container. There would be no manifest screening and non-intrusive scanning. A team of customs officials would open every container upon its arrival to the port (via land

or transshipment), and visually inspect the container cargo. The teams would carry portable radiation detectors and use dogs to detect explosives and chemicals. After the team verifies the cargo is legitimate, the container would be sealed and loaded onto the container ship. There would be no data sharing and use of smart tags.

2. System Design Attributes

Source ports are located in areas of a country that usually have direct deep water access to the shipping lanes of the world. In addition, areas around source ports tend to be congested by the infrastructure and related industries that burgeon in the local vicinity of a source port. The location and scarcity of available space constrains the design space to one in which careful consideration must be given prior to the recommendation of alternatives that would further limit the port space or restrict future operations or limit the ports container throughput. Alternatives that have a combination of acceptable performance while minimizing the impact on port operations, cost, space, and resource allocation will have an advantage over other better performing alternatives. The development of alternatives that require large footprints for housing scanning equipment or that require large or many support facilities will not be supported by the majority of the stakeholders due to the limited design space. The design space is not only limited by the physical constraints and boundaries of the port itself, the city and country in which it resides, but also by local, federal, and international laws that govern legitimate free trade between cooperating countries. For example, the Container Security Initiative 2006-2011 Strategic Plan, published by CBP contains many initiatives and future policies that will be levied against source ports that will have to comply with those constraints [51]. The addition of local, state, federal, and international laws in the design space for alternative generation is essential in ensuring that the alternatives generated will be acceptable for current and future implementation.

3. Feasibility Screening

The purpose of feasibility screening is to evaluate alternatives that clearly do not meet the system requirements. There are eight criteria used for the feasibility screening. Foremost, the system must be able to detect chemical, biological and radiological

weapons. Every non-intrusive screening station should be manned by at most two personnel and each scanning should not take more than one minute. From the health perspective, the radiation exposure for the operator should be less than 10 mrem annually. Each screening station should not take up more than 100 square meters. The technology has to be available and system to be ready to be fielded by 2012.

The first alternative to be removed is the zero percent screening. Although this will have little economic impact and will not delay the cargo, the system will not be able to detect chemical, biological, radiological and explosive material before the container is loaded onto the container ship. The zero percent screening alternative fails to meet this main requirement and it is removed from consideration.

The second alternative to be removed from consideration is the 100 percent intrusive inspection. The sheer manpower needed to physically inspect each and every container is enormous and not cost effective. The delays caused by the intrusive inspection per container would be up to eight hours and it is not economical to implement the procedure [52]. The physical and economic constraints render the 100 percent intrusive inspection to be ineffective.

The high performance alternative utilizes several screening technologies. System requirements cannot be met if fewer than two personnel are employed for non-intrusive screening. SSTG concluded that the manpower required for dog handlers, drivers for the mobile screening vans and other additional manpower support to run the system was greater than two.

The alternatives that passed the feasibility screening are Improved Loading Search, Minimal Port Operations Search, and 100 percent volume screening. These alternatives all passed the basic requirements, except for the status quo, which failed the requirement to detect chemical weapons non-intrusively. SSTG decided to keep status quo for modeling and simulation in order to have a baseline reference to view if the alternatives improve the overall performance. Table 50 shows the overall results of the feasibility screening for the seven alternative designs.

	Manpower required is less than 2 per non- intrusive screening	Operational NLT 2010	Total Time per container less than 1 minute for non- intrusive scan	Equipment Footprint Less Than 100 Square Meters	Operator Exposure less than 10urem/year	Capability to detect Chemical Weapons Non- Intrusive	Capability to detect Biological Weapons	Capability to detect Radiological Weapons	RECAP
Status Quo	G	G	G	G	G	NG	G	G	NG
0% Inspection	G	G	G	G	G	NG	NG	NG	NG
100% Inspection (100% of the containers)	G	G	G	G	G	G	G	G	G
Improved Loading Search	G	G	G	G	G	G	G	G	G
Minimum Port Operations Disruption	G	G	G	G	G	G	G	G	G
High Performance	NG (~dog handlers?)	G	G	G	G	G	G	G	NG
100% Intrusive Inspection	NG	G	NG	NG	G	G	G	G	NG

Table 50. Deny Loading of Undesired Cargo Feasibility Screening

C. MODELING AND ANALYSIS

1. Modeling Plan

The SSTG used EXTEND version 6.0 to model the workflow of the containers arriving at the port, the screening and inspection stations and ending at the loading bay. One model was created to represent the workflow while the alternatives were modeled by varying the different factors. A total of 17 factors were identified for the analysis. The different combinations of these 17 factors describe different sensor suite configurations that were analyzed for overall inspection performance and effectiveness.

The scale of the 17 factors of interest would require no less than 2^{17} runs to investigate the effects of various combinations. The sheer magnitude of our experiment requires intelligent design of experiments in order to maximize potential information and data analysis with the minimal number of experiments. Cioppa describes a way to generate smart design of experiments using the Nearly Orthogonal Latin Hypercube (NOLH) algorithm [53]. A NOLH design spreadsheet created by Sanchez combined several works to create a user-friendly Microsoft Excel worksheet that allowed convenient input of factors to get the optimal design of experiments [54]. The team also explores an Extended NOLH algorithm by Ang to investigate the better experiment design for simulation runs [55]. With the NOLH algorithms, the original 2^{17} runs can be reduced to 129 or 65 runs if the NOLH or ENOLH algorithm was to be used respectively.

The model is built to answer two MOEs of accuracy of container screening and timeliness. These MOEs are quantified by MOPs.

The following MOPs are measured to evaluate the accuracy MOE.

- MOP: Probability of detecting undesired cargo
- MOP: Probability of Miss Detection
- MOP: Probability of False Alarm

The following MOPs are measured to evaluate the timeliness MOE.

- MOP: Average handling time per container
- MOP: Container throughput

The objective of the analysis was to determine the different mixes of alternatives in each inspection station and their effects on the MOP. The Type I and Type II errors were carefully considered and depicted in Table 51.

Sensors Output	Null Hypothesis: Container is Dirty	Actual Container Condition	
		Dirty	Clean
	Fail	Correct Detection	False Alarm (Type II error β)
	Pass	Miss Detection (Type I error α)	Null Event

Table 51. SSTG Type I and II Errors Defined

2. Modeling Explanation

The scenario of interest was a flood of dirty containers that are planted by terrorists to be shipped on three US-bound ships. The simulation modeled port inspection operations to foil the terrorists' objectives in this scenario within a 12-hour period. The performance metrics of the study were built upon the statistics of the various inspection processes and in particular, the success of the terrorists' objectives. The entire port inspection model was summarized by its five key components.

- Container Generation
- Fixed point of entry
- Holding yard (non-intrusive) inspection
- Intrusive Inspection
- Crane (non-intrusive) Inspection

The simulation model to examine the five key components listed above is depicted in Figure 106.

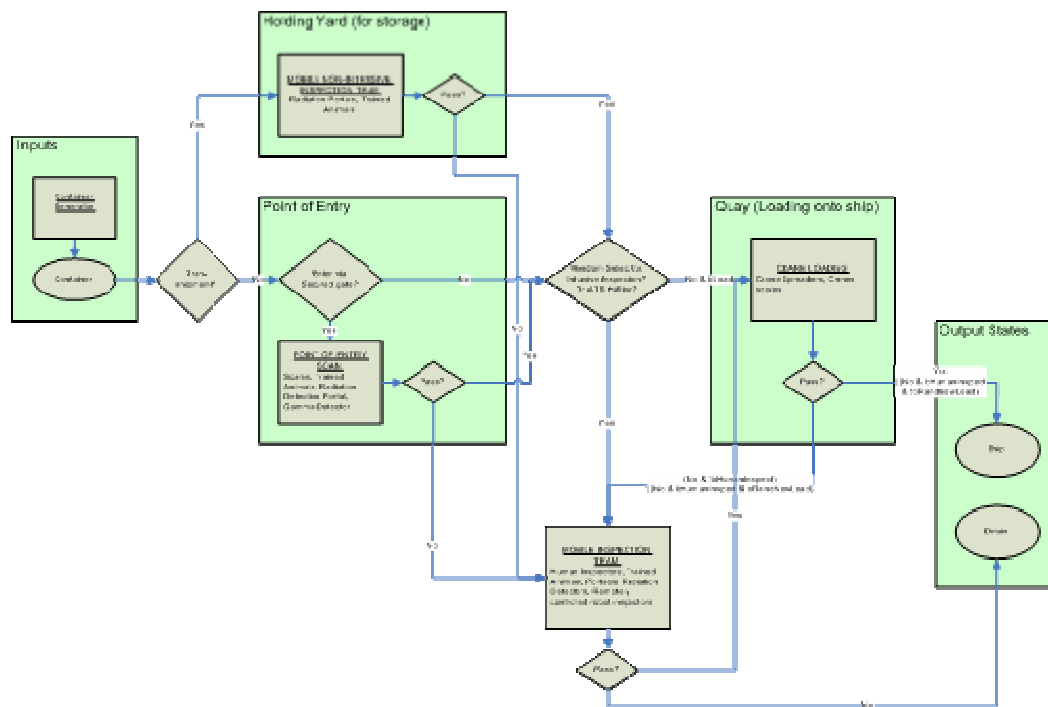


Figure 106. SSTG Simulation Model

a. General Flow of Containers through Port Inspections

Incoming containers into the source port were handled differently according to their mode of arrival: sea and land.

The bulk of containers in the model were transshipment containers, which arrive via the sea and were temporarily stored in our source port (acting as intermediary for these transshipment containers) holding yard for 3-5 days before transferred onto another ship bound for its final destination [56]. There are mobile inspection machines patrolling the holding yard to inspect transshipment containers while they were in transit.

Other incoming containers arrived via land either by truck or rail. These land containers were scheduled in a just-in-time fashion so that they arrived at the source port on the day of loading and were routed immediately to the loading bay after clearing inspections at the point of entry.

If a source port was equipped with ATS risk profiling, the manifests of all incoming containers would have undergone risk profiling prior to the physical arrival of the containers. Those containers that were profiled as high-risk were picked out for intrusive inspection before loading onto the departing ship. A second level of random selection for intrusive inspection was also in place to randomly check containers regardless of their risk profile and origin.

Cleared containers were routed to the quay for loading when they undergo the last level of inspections while being loaded by the quay-side cranes.

All dubious or dirty containers that failed at the various levels of inspection were sent to the intrusive inspection teams for thorough examination. Dirty containers when found by the intrusive inspection teams were detained for further handling by the relevant authorities.

b. General Assumptions for All Inspection Modules

Throughout the entire model, containers were categorized as “clean” and “dirty” in the model. A dirty container was one that was planted by the terrorist and contains undesired cargo. The nature of the undesired cargo was randomly selected as nuclear, biological or chemical. On the other hand, a clean container was one that is legitimately being shipped for commerce purposes and does not hold any undesired cargo.

For all inspection modules, there was more than one sensor. The model requires passes from all sensors for a container to be cleared as “clean”. Thus if any sensor fails the container, the container would be suspected of being “dirty”.

For all inspection modules, each container underwent all sensors. Inspection did not stop at the earliest point of clearance failure. For example, the fixed point of entry may be equipped with scales, trained animals, radiation detectors and gamma scanners in this particular order of inspection. If the animals signal dubious content, the container was sent to the radiation detector and gamma scanner respectively before sent to the intrusive inspection team. Proceeding with the full set of inspections

will enable quicker and better informed diagnostics at the intrusive inspection team, as well as minimize disruption of the processing flow.

The point of entry, holding yard and quay-side crane inspection were single-queue-multiple-servers model. The intrusive inspection is a priority-queue-multiple-servers model.

c. Process Flow for Container Generation

There were two container generators, one for each mode of arrival: truck and sea. The truck container generator assumed a constant arrival rate for container at source port. The transshipment container generator creates a fixed amount of transshipment containers (equivalent to transshipment volume shipped per day) and this transshipment container population remains constant for the rest of the 12-hour simulation. The model does not model the influx of transshipment containers as transshipment containers are expected to spend days within the simulated source port and hence arriving transshipment containers within the simulated 12-hour time frame are not due for re-shipping anytime soon. Thus they are not included for simulation.

Dirty containers containing explosive contents are planted among the legitimate containers. These containers are designated to contain either unwanted cargo that is radioactive, biological or chemical in nature.

Upon leaving the container generation module, each container was routed to a different path according to its arrival mode: transshipment container that arrived via sea was routed to the holding yard and land containers that arrived via truck or rail were routed to the point of entry gates.

d. Process Flow for Fixed Point of Entry

The model simulated a port with multiple entry points, with only a certain percentage of entry points fitted with all sensors. The land containers were randomly selected to enter the sensor gates and non-sensor gates. Each of these sensors were characterized by inspection time, probability of detection and false alarm rate.

Land containers that enter via non-sensor gates were cleared for this stage of inspections. Land containers that enter via sensor gates went through one or more of these non-intrusive sensors. Containers that do not pass this stage of inspection were sent for intrusive inspection.

e. Process Flow for Yard (Non-Intrusive) Inspection

The model simulated one central holding area with several mobile inspection machines that roamed the holding yard and scanned the containers while they were in transit. The mobile inspection machine was characterized by its service time, inspection time, probability of detection and false alarm rate.

Containers that were in the holding area for a time shorter than the mobile inspection machines' service time did not get inspected and were cleared for this stage of inspections. Containers that did not pass this stage of inspection were sent for intrusive inspection.

f. Process Flow for Crane (Non-Intrusive) Inspection

The model simulated multiple quay cranes loading containers onto each ship. Each of the quay cranes was equipped with either one or both of the radiation detector and gamma scanner. These scanners inspect the container while it was being transferred from the quay to the ship. For some containers, this was the only stage of inspection as they may have skipped inspections at the point of entry or holding yard.

Containers that failed either sensor were handled differently based on their history of inspections in the port. The following handling rule-set was partially derived from understanding of port operations at Port of Oakland [57].

- Suspected containers that have not undergone any previous inspections are immediately lowered back on the quay and taken away for intrusive inspection with high priority so that it can be processed on time for loading.
- Suspected containers that have previously triggered a similar sensor but was previously cleared would be treated as cleared on the quay sensor. An example would be a container of ceramic tiles with some natural radiation triggers the radiation detection at the point of entry and was cleared. When

it triggers the radiation detector on the loading crane, it would be treated as cleared and loaded.

- Suspected containers that trigger the crane sensor for the first time would be treated as failed on the quay sensor and immediately lowered back on the quay and taken away for intrusive inspection with high priority for loading. An example would be the same container in the previous paragraph triggering the gamma sensor on the crane but not triggering gamma sensor at the holding yard or point of entry.

g. Process Flow for ATS and Random Inspection

The ATS and random selection processes singled out containers for intrusive inspection on a systematic and random manner respectively.

The model simulated two efficiency levels of ATS: namely default ATS and ATS plus. The difference between both ATS levels would be their ability to single out high risk containers for inspection. In the model, dirty containers were flagged as high-risk with a higher probability than clean containers. For the default efficiency level of ATS, 6 percent of all containers were marked high risk and 12 percent of dirty containers were marked high risk. For the higher efficiency level of ATS plus, 6 percent of all containers were marked high risk and 18 percent of dirty containers were marked high risk.

The model simulated a random percentage between 0 to 10 percent of all containers being selected for intrusive inspection.

The above processes sent a regular stream of containers to the intrusive inspection team.

h. Process Flow for Intrusive Inspection

The intrusive inspection team received high-risk containers from ATS risk-profiling, random containers selected and containers that had been failed by the crane sensors.

Intrusive inspection teams consisted of human operators who were aided by the following sensors: trained animals, radiation detectors, gamma scanners, biological detectors and chemical detectors. Intrusive inspection was characterized by

service time, inspection time, and probability of detection. A pass status for this stage of inspection would allow a container to be loaded onto the ship despite further triggering of the crane sensors. A failed status for this stage will cause the container to be detained.

The model can detain a clean container without finding dirty contents within a stipulated inspection time. This is with consideration that the intrusive inspection has to be highly efficient and constrained within 30 minutes to handle the large flow of containers. Thus clean containers that repeatedly trigger off the sensors wrongly are deemed to be suspicious and inappropriately pre-declared. Thus they are detained and the associated economic cost to be borne by the shipper.

The number of inspection teams is set at 15 in the model. This is based on pre-known statistics that ATS selects 6 percent of all containers for intrusive section and random selection of containers is set at 0 to 10 percent. This huge volume of containers selected for intrusive inspection warrants the adequate supply of inspection teams to ensure smooth port operations. 15 teams is a reasonable figure computed from the container traffic and 30 minutes average inspection time per container. When more containers are sent for intrusive inspection due to false alarm of sensors, we expected these teams to be further loaded.

3. Model Inputs

a. Container Traffic

The port statistics of container volume in the model is modeled after statistics of the PSA Singapore Terminals, the world's largest transshipment hub. PSA Singapore handled 22.3 million TEUs of (transshipment) containers in 2005 and this transshipment volume made up 95 percent of Singapore's total throughput of 23.2 million TEUs. A 2002 Spring Singapore publication describes a typical day at PSA (Year 2000) would see 60 ships berthing and un-berthing with 47,000 containers moved and 8,000 trucks passing through its gates [58]. The PSA Annual Report 2005 describes the "scale of PSA in Singapore. 41 berths, 131 quay cranes, and four seamlessly integrated world-class container terminals in one location link shippers to an excellent network of 600 ports in 123 countries via 200 shipping lines [59]"

The following statistics (deduced average PSA container traffic) are obtained from the above information by simple averaging.

- 15000 TEUs of transshipment containers per day per terminal
- 800 TEUs of incoming (truck) containers per day per terminal
- Berth/unberth 15 ships using 33 cranes along its ten berths

From the information gathered, the model will simulate an “example terminal” approximately a-third the scale of a PSA terminal and for a 12-hour time frame. As we are obtaining statistics from the world’s busiest port, as well as biggest transshipment hub, the container traffic will be further moderated by a 25 percent reduction for realism. The container traffic of the simulated terminal will be as follows:

- 1875 TEUs of transshipment containers within 12 hours
- 100 TEUs of incoming (truck) containers within 12 hours
- Berth/unberth 5 ships using 11 cranes

b. Sensor Performance

Sensors are modeled by their probabilities of detection and false alarm. While efforts have been made to research on the required probabilities, there have been few results. Hence the model will assume that future technology will catch up and adequate sensors will be fielded by 2012 with the following desired probabilities of detection and false alarm. Table 52 through 55 describes the sensor performance inputs for fixed entry, non-intrusive inspection, intrusive inspection, and cargo locations.

Location: Fixed Entry Data Array: gfEntry	Scales	Animals	Radiation Detector (Passive)	Gamma Scanner (Active)	Biological detector	Chemical detector
Possibility	1	1	1	1	0	0
P_{FA}	0.01	0.01	0.01	0.01	0	0
P_{Detect} against radioactive material	0	0	0.9	0.5	0	0
P_{Detect} against biological material	0	0	0	0.5	0	0
P_{Detect} against chemical material	0	0.5	0	0.5	0	0
P_{Detect} against explosive material	0	0.8	0	0.8	0	0

Table 52. Sensor Performance Inputs for Fixed Entry

Location: NonIntrusive Inspection Data Array: gfHolding	Scales	Animals	Radiation Detector (Passive)	Gamma Scanner (Active)	Biological detector	Chemical detector
Possibility	0	0	1	1	0	0
P_{FA}	0	0	0.01	0.01	0	0
P_{Detect} against radioactive material	0	0	0.9	0.5	0	0
P_{Detect} against biological material	0	0	0	0.5	0	0
P_{Detect} against chemical material	0	0	0	0.5	0	0
P_{Detect} against explosive material	0	0	0	0.8	0	0

Table 53. Sensor Performance Inputs for Non-Intrusive Inspection

Location: Intrusive Inspection Data Array: gfIntrusive	Scales	Animals	Radiation Detector (Passive)	Gamma Scanner (Active)	Biological detector	Chemical detector
Possibility	0	1	1	1	1	1
P_{FA}	0	0.01	0.01	0.01	0.01	0.01
P_{Detect} against radioactive material	0	0	0.9 [60]	0.5	0	0
P_{Detect} against biological material	0	0	0	0.5	0.7	0
P_{Detect} against chemical material	0	0.5	0	0.5	0	0.7
P_{Detect} against explosive material	0	0.8	0	0.8	0	0

Table 54. Sensor Performance Inputs for Intrusive Inspection

Location: Crane Data Array: gfCrane	Scales	Animals	Radiation Detector (Passive)	Gamma Scanner (Active)	Biological detector	Chemical detector
Possibility	1	0	1	1	0	0
P_{FA}	0.01	0	0.01	0.01	0	0
P_{Detect} against radioactive material	0	0	0.9	0.5	0	0
P_{Detect} against biological material	0	0	0	0.5	0	0
P_{Detect} against chemical material	0	0	0	0.5	0	0
P_{Detect} against explosive material	0	0	0	0.8	0	0

Table 55. Sensor Performance Inputs for Crane

4. Model Results and Analysis

This section of the report contains the data analysis of the raw output data that was generated from the SSTG Extend model. The first section will detail the type of data that was generated from the Extend model, define key terminology associated with the model and explain how the Measures of Performance were calculated from the generated data. A logistic linear regression model was fit to the data to help to interpret the meaning of the model output and to help predict future values of how varying a randomly

selected percentage of containers to be inspected could affect the probability of detection. The logistic regression model was only fit to the probability of detection MOP and therefore another technique was used to interpret the results of the other MOPs and to also reinforce the results of the logistic regression model with respect to the probability of detection MOP.

Partitioning analysis was used as an intuitive analytical tool to interpret the results of the output data for the remaining MOPs. An easy to ready flow chart instantly showed the results of taking out or leaving in sensors on the impact of the MOP under study.

a. Optimal Sensor Mix

The optimal sensor mix was a combination of gamma scanners on the crane spreaders and holding area combined with all available sensors at the inspection station including the gamma scanner, radiation detector, chemical, biological detectors, and animals trained in detection. The radiation detector in the holding area was also considered significant.

SSTG Extend Model Logistic Regression Data Analysis

The SSTG Extend model has been discussed in great detail in both the construction of the model and the individual model components. The actual raw data output that was generated from that model is included in the SSTG Data Analysis Appendix. The type of output generated allows the user to analyze the overall impact on average container throughput per hour as well as the overall detection capability of the system. The raw data was used to calculate our Measures of Performance as well as to capture predictor and response variables for linear regression. The sensors that were used for the detection of the dirty containers were located at four different locations and were modeled accordingly in Extend.

When the Extend model was run, it produced performance data for each station. An example of what type of data that was generated is included below. Table 56 shows the general format of the Extend model output for each station for collecting the Measures of Performance related to accuracy.

Inspection Station (Por. of Entry, Holding Area, Inspection Station, Loading Area)							
Clean container Arrived	Dirty Container Arrived	Clean Container Start Insp	Dirty Container Start Insp	Clean Container Passed	Dirty Container Passed	Clean Container Failed	Dirty Container Failed

Table 56. Station Format for Determining MOP Related to Accuracy

- Clean Container Arrived – Count of the number of clean containers that arrived at applicable station.
- Dirty Container Arrived – Count of the number of dirty containers that arrived at the applicable station.
- Clean Container Start Inspection – Count of the number of clean containers that began the inspection process at the applicable station.
- Dirty Container Start Inspection – Count of the number of dirty containers that began the inspection process at the applicable station.
- Clean Container Passed- Count of the number of clean containers that passed the inspection and have completed the entire inspection process at the applicable station.
- Dirty Container Passed- Count of the number of dirty containers that made it through the inspection process without detection (Missed Detection).
- Clean Container Failed- Count of the number of clean containers that failed the inspection at the applicable station and were either sent to the Intrusive inspection station or detained if already at the intrusive inspection station.
- Dirty Container Failed – Count of the number of dirty containers that failed the inspection at the applicable station and were either sent to the Intrusive inspection station or detained if already at the intrusive inspection station.

Table 57 shows the general format of the Extend model output for each station for collecting the Measures of Performance related to timeliness.

Inspection Center					
Container Arrived	Container Serviced	Utilization	Average Queue Length	Average Queue Time	Average Total Time
304	56	0.999999	160.6202	21004.29	22879.72

Table 57. Station Format for Determining MOP Related to Timeliness

- Container Arrived- Count of the number of containers that arrived at applicable station

- Container Serviced- Count of the number of containers that were serviced at the applicable station.
- Utilization- Amount of time that the service station was occupied with customers during the simulation run time interval. For example, the inspection center was occupied with customers for a total of 8 hours out of the 12 hours of simulated run time, resulting in an utilization rate of .67.
- Average Queue length – Average number of containers waiting in line to be serviced.
- Average Queue time- Average amount of time the containers spent in the Queue (measured in seconds).
- Average Total Time- Average amount of time a container spent at the service station. This time includes Queue time and service time.

Measures of Performance Related to Accuracy

The probability of detecting undesired cargo was calculated by summing the total number of dirty containers that had been detained and dividing that number by the total number of containers that had been processed by the system. The Extend model default was to generate 12 dirty containers, however not all of those containers were necessarily processed by the system before the 12 hour run time has expired. Some containers could be in the queue or were still being serviced at any 1 of the 4 stations when the simulation had ended. The Probability of detection was calculated from the raw data by the following formula:

$$\frac{\text{dirty_containers_held}}{\text{dirty_containers_held} + \text{dirty_containers_loaded}}$$

The probability of a missed detection was calculated by counting all of the dirty containers that passed through all of the inspection stations and was loaded onto the ship divided by the total number of dirty containers that had been processed by the system. The probability of a missed detection was calculated from the model raw data output by the following formula:

$$\frac{\text{dirty_containers_loaded}}{\text{dirty_containers_loaded} + \text{dirty_containers_held}}$$

The probability of a false alarm was calculated by counting the total number of clean containers that were being detained divided by the total number of clean containers that had been processed by the system. The probability of false alarm was calculated from the model raw data output by the following formula:

$$\frac{\text{clean_containers_held}}{\text{clean_containers_loaded} + \text{clean_containers_held}}$$

Measures of Performance Related to Timeliness

The average handling time per container was calculated by multiplying the total number of containers that arrived at each handling station, where sensors were located, by the total average time spent at each station. This produced the total amount of processing time per station. The processing time for each station was summed and then divided by the total number of containers that was processed by all of the inspection stations. This gave the average processing or handling time per container.

Total service time at Entry = (# of Containers serviced at Entry)*(Entry average time) (1)

Total service time at Yard = (# of Containers serviced at Yard)*(Handling average time) (2)

Total service time at Customs = (# of Containers serviced at Customs)*(Customs average time) (3)

Total service time at Crane = (# of Containers serviced at Crane)*(Crane average time) (4)

$$\frac{(1) + (2) + (3) + (4)}{\text{Total_}\#\text{_containers_processed}}$$

Container throughput was be measured by the total number of containers processed per hour. The formula used from the model raw data output was:

$$\frac{3600 * (\text{Clean_Containers_loaded} + \text{Dirty_Containers_Held})}{\text{Total_Model_Runtime(Seconds)}}$$

SSTG Raw Data Linear Regression

The Extend Model raw data was outputted into Microsoft Excel spreadsheet and then expanded into a new data set to include the MOP for linear regression analysis in S-Plus version 7 and Minitab version 14. The data set compilation was automated through the use of a MatLab program. The complete data set was

imported into S-Plus and a logistic linear regression model with the logit link function was used to fit a model to the generated data.

The analyzed response variable was the probability of detection of a container loaded with undesired cargo, as detailed in the earlier sections of the report, by a terrorist organization. The terrorists flooded the port with 12 dirty containers with the goal to have 3 of the 12 dirty containers loaded onto a ship bound for the United States. The probability of detection was calculated using the formula as detailed above, but the logistic regression model with a logit link function from the binomial family works best when the response variable is a success or failure (0 or 1). In order to provide the correct 0 or 1 response variable for the statistical software package, the data set had to be expanded to include a field for detected or not detected. The Extended Nearly Orthogonal Latin Hypercube (ENOLH) Matrix as outlined in earlier sections of the report generated 65 different configurations in order to provide efficient space filling and reducing the possibility of multicollinearity. Each configuration was run through the model 10 times to generate 10 observations for each configuration. This resulted in 650 total observations. However, in order to capture which containers were detected and which containers were not detected, each configuration had to be expanded by the total number of dirty containers processed. The total number of containers detained was already a generated numerical output and that numeric output was used to randomly assign an equivalent number of containers with a 1 indicating that they had been detected. This procedure was performed on the Extend output data by a MatLab routine. The data set response variable is now coded properly for the logistic regression model.

The regressors or predictor variables for this model were all of the different sensors that were used to determine whether or not a container was dirty or clean. The following is a list of predictor variables:

- eScales(es)- Scales that were used for weighing containers at the port of entry that were brought into the port by trucks. This regressor is a categorical variable with values of 0 and 1. A value of “0” indicates that the sensor is “off” and not in the system. A value of “1” indicates that the sensor is “on” and is part of the system.
- eAnimals(ea)- Trained animals at the port of entry to detect particular chemical compounds. This regressor is a categorical variable with

values of 0 and 1. A value of “0” indicates that the sensor is “off” and not in the system. A value of “1” indicates that the sensor is “on” and is part of the system.

- eRad(er)- Radiation detector at the port of entry to detect radiation levels above a preset threshold level at the port of entry. This regressor is a categorical variable with values of 0 and 1. A value of “0” indicates that the sensor is “off” and not in the system. A value of “1” indicates that the sensor is “on” and is part of the system.
- eGamma(eg)- X-Ray, Gamma ,or Neutron scanner used to scan container contents at the port of entry (Fixed Scanner). This regressor is a categorical variable with values of 0 and 1. A value of “0” indicates that the sensor is “off” and not in the system. A value of “1” indicates that the sensor is “on” and is part of the system.
- hRad(hr)- Radiation detector used at the holding area to detect radiation levels above a threshold level in the holding area. This regressor is a categorical variable with values of 0 and 1. A value of “0” indicates that the sensor is “off” and not in the system. A value of “1” indicates that the sensor is “on” and is part of the system.
- hGamma(hg)- X-Ray, Gamma, or Neutron scanner used to scan container contents in the holding area (Mobile Scanner). This regressor is a categorical variable with values of 0 and 1. A value of “0” indicates that the sensor is “off” and not in the system. A value of “1” indicates that the sensor is “on” and is part of the system.
- iAnimals(ia)- Trained animals used to detect particular chemical compounds at the intrusive inspection area. This regressor is a categorical variable with values of 0 and 1. A value of “0” indicates that the sensor is “off” and not in the system. A value of “1” indicates that the sensor is “on” and is part of the system.
- iRad(ir)- Radiation detector used to detect radiation levels above a threshold level at the intrusive inspection station. (Portable device) This regressor is a categorical variable with values of 0 and 1. A value of “0” indicates that the sensor is “off” and not in the system. A value of “1” indicates that the sensor is “on” and is part of the system.
- iBio(ib)- Biological agent detector used to detect suspect biological agents in containers at the intrusive inspection station (Mobile). This regressor is a categorical variable with values of 0 and 1. A value of “0” indicates that the sensor is “off” and not in the system. A value of “1” indicates that the sensor is “on” and is part of the system.
- iChem(ic)- Chemical compound detector used to detect certain chemical compounds in containers at the intrusive inspection station (Mobile) This regressor is a categorical variable with values of 0 and 1. A value of “0” indicates that the sensor is “off” and not in the system. A value of “1” indicates that the sensor is “on” and is part of the system.

- cScales-(cs) Weight scales attached to the crane spreaders where transshipment cargo is loaded onto waiting ships. This regressor is a categorical variable with values of 0 and 1. A value of “0” indicates that the sensor is “off” and not in the system. A value of “1” indicates that the sensor is “on” and is part of the system.
- cRad(cr)- Radiation detector used to detect container radiation levels above a preset threshold level on the crane spreader. This regressor is a categorical variable with values of 0 and 1. A value of “0” indicates that the sensor is “off” and not in the system. A value of “1” indicates that the sensor is “on” and is part of the system.
- cGamma(cg)- X-Ray, Gamma, and/or Neutron Scanner used to detect suspicious objects in containers located on the crane spreader. This regressor is a categorical variable with values of 0 and 1. A value of “0” indicates that the sensor is “off” and not in the system. A value of “1” indicates that the sensor is “on” and is part of the system.
- ATS(ats)- Automated Tracking System used to identify suspicious containers through legal documentation and manifest. Values of 0 indicate that ATS is not used. A value of “1” indicates that the basic ATS is used and in the system. A value of “2” indicates that the enhanced ATS system is used and in the system.
- eScanPrc(esp)- Entry scan percentage. The entry scan percentage is based upon that percentage of containers that are arriving by trucks that will be subjected to the sensors at the port of entry. The reason behind varying the percentage of scanned trucks is to allow the modeler to model a port that is in various states of construction where there are multiple entry gates or entry lanes where all gates or lanes do not have scanning sensors. For example, a port with 2 entry gates or 2 lanes at one gate may have 1 gate where all trucks are subjected to scanning, but the other gate does not have the equipment installed. The scanning percentage for this configuration would be .5 or 50%.
- iRdmSel(irs)- Random Selection. The percentage of containers that are randomly selected for intrusive inspection can be set to any user selected percentage from 0-10% to determine the effect that random selection has on the Measures of Performance.

The general format for the Logistic Linear Regression model was as follows:

$$Y_i \sim \text{Binomial}(n_i = 1, \pi_i)$$

$$\text{where } \pi_i = \text{probability_of_success} = E(Y_i)$$

The general form of the logistic model was:

$$\ln\left(\frac{\pi_i}{1-\pi_i}\right) = \beta_0 + \beta_1 x_i + \dots + \beta_k x_k$$

The expected value of the response variable was:

$$E(Y_i) = \pi_i$$

The variance of the response variable was:

$$Var(Y_i) = \pi_i(1 - \pi_i)$$

Fitting our parameters into the general model without 2 way interactions would lead to the following model:

$$\ln\left(\frac{\pi_i}{1-\pi_i}\right) = \beta_0 + \beta_{es}x_{es} + \beta_{ea}x_{ea} + \beta_{er}x_{er} + \beta_{eg}x_{eg} + \beta_{hr}x_{hr} + \beta_{hg}x_{hg} + \beta_{ia}x_{ia} + \beta_{ir}x_{ir} + \beta_{ib}x_{ib} + \beta_{ic}x_{ic} + \beta_{cs}x_{cs} + \beta_{cr}x_{cr} + \beta_{cg}x_{cg} + \beta_{ats}x_{ats} + \beta_{esp}x_{esp} + \beta_{irs}x_{irs}$$

The above model was run in S-Plus and the summary results of the model in the form of a deviance table and summary statistical data is included in the SSTG Appendix for Model Data Analysis. A likelihood ratio test was performed to test the above model with the saturated model and the result of that test was a p-value that was equal to zero. This implies that at least one of the regressor variables in the logistic regression model is important because it has a non-zero regression coefficient. Table 58 presents the result of Goodness of Fit Test.

Method	Chi-Square	DF	P
Pearson	755.598	47	0.000
Deviance	737.092	47	0.000
Hosmer-Lemeshow Brown:	156.758	8	0.000
General Alternative	7.599	2	0.022
Symmetric Alternative	4.676	1	0.031

Table 58. Results of Goodness of Fit Test

Table 59 presents the Type III Sum of Squares for the 17 factors. The p-values are indicating that the scales at the point of entry and on the crane are not significant in determining whether or not a container will be detected or not detected. In addition, the animals at the point of entry are not significant whereas the animals at the inspection station are a factor. This could be due to the fact that in our model the majority of the containers went through the transshipment hub and therefore many more containers were inspected by the animals at the inspection station than at the point of entry.

	Df	Sum of Sq	Mean Sq	F Value	Pr(F)
eScales	1	0.0328	0.03280	1.063	0.3026147
eAnimals	1	0.0497	0.04972	1.611	0.2044145
eRad	1	0.0017	0.00175	0.057	0.8118064
eGamma	1	0.3797	0.37966	12.301	0.0004554
hRad	1	0.8625	0.86251	27.945	0.0000001
hGamma	1	17.5407	17.54069	568.301	0.0000000
iAnimals	1	14.5561	14.55610	471.603	0.0000000
iRad	1	1.6846	1.68458	54.579	0.0000000
iGamma	1	22.0935	22.09345	715.806	0.0000000
iBio	1	1.3446	1.34461	43.564	0.0000000
iChem	1	0.9106	0.91059	29.502	0.0000001
cScales	1	0.0014	0.00143	0.046	0.8293453
cRad	1	0.0017	0.00168	0.054	0.8154716
cGamma	1	32.8884	32.88835	1065.550	0.0000000
ATS	1	0.3262	0.32616	10.567	0.0011561
eScanPrc	1	0.1976	0.19760	6.402	0.0114188
iRdmSelPrc	1	0.0524	0.05239	1.697	0.1926548

Table 59. Type III Sum of Squares for the 17 Factors

There were 12 dirty containers generated by the model and only two were selected to come into the port through the port by way of truck and the other 10 were brought into the port by way of transshipment. The radiation detector at the port of entry and on the crane spreader also had large p-values indicating that they were not significant in detecting or not detecting the dirty containers. This was likely due to the fact that the detectors probability of detecting one certain type of radiation combined with the fact that only four out of the 12 dirty containers were loaded with radioactive material, and out of

the 12 containers only two were loaded to come into the port through the port of entry, resulting in a low level of significance in identifying dirty containers. The radiation detector at the inspection team had a low p-value implying that it was significant in detecting or not detecting the dirty containers. The fact that any container that was flagged by any of the inspection stations or randomly selected will be sent to the intrusive inspection team, making it much more likely that all of the sensors at the inspection station to encounter a dirty container. This was the reason that all of the sensors at the inspection station had a high level of significance.

In order to predict how the random selection percentage affects the probability of detection, the linear regression model can be used. The randomly selected percentages can be set as a variable from 0 to 100 percent and determine a probability of detection based upon the configuration of sensors that are selected.

The Akaike Information Criterion (AIC) algorithm was used to determine the significant regressors for inclusion in the logistic regression model. The summary of S-Plus output is included in Table 60. This algorithm is a well known procedure that is more mathematically rigorous and methodical at eliminating regressors than simple backwards elimination or inspection of the p-values. The model returned by step AIC is:

```
glm(formula = Detected ~ eGamma + hRad + hGamma + iAnimals + iRad +  
iGamma + iBio + iChem + cScales + cGamma + ATS + eScanPrc
```

Coefficients:

Intercept	eGamma	hRad	hGamma	iAnimals	iRad	iGamma
-3.039303	0.2130138	0.2805187	1.238218	1.293522	0.4795299	1.582345

Degrees of Freedom: 7787 Total; 7774 Residual
Residual Deviance: 7513.159

iBio	iChem	cScales	cGamma	ATS	eScanPrc
0.3970485	0.311408	0.09136354	1.927764	-0.08831393	0.1965489

Table 60. Coefficients and Results of the stepAIC Function

Mallow's Cp was calculated for the full model with ATS, eScanPrc, and iRdmPrc to determine which was the best subset that would include these particular regressors to predict which percentage of random scanning selection, ATS level, and intrusive inspection random selection that would return the highest Probability of detection. The subsets with their Mallow's Cp are shown in Figure 107. It is interesting to note that the different methods all pointed to models with the same regressors with the exception that Mallow's Cp did not determine the cScales to be important whereas the stepAIC did. This could be due to the fact of the extra restriction that was placed on the Mallow's Cp generation of including ATS, eScanPrc, and iRdmPrc. The inclusion of these regressors could have minimized the significance of the cScales regressor.

					E i e A A S n e h n I S c c I G G I G I c G a m e a h a m I a I C a c a l a R m R m a R m B h l R m e l a m a m l a m I e e a m s s d a d a s d a o m s d a												
Vars	R-Sq	R-Sq(adj)	Mallows C-p	S													
1	10.8	10.8	1799.8	0.44885													
1	7.4	7.4	2163.9	0.45730													
2	17.7	17.6	1065.5	0.43128													
2	15.2	15.1	1334.8	0.43780													
3	22.2	22.2	579.8	0.41924													
3	22.0	22.0	599.9	0.41974													
4	26.4	26.4	130.5	0.40778													
4	22.9	22.8	512.8	0.41753													
5	27.1	27.0	60.8	0.40595													
5	26.8	26.7	92.0	0.40676													
6	27.5	27.4	23.5	0.40496													
6	27.2	27.1	53.6	0.40574													
7	27.6	27.5	15.6	0.40473													
7	27.5	27.4	19.8	0.40484													
8	27.6	27.5	11.3	0.40459													
8	27.6	27.5	14.7	0.40468													
9	27.6	27.5	10.5	0.40454													
9	27.6	27.5	12.2	0.40459													
10	27.7	27.5	11.4	0.40454													
10	27.6	27.5	11.8	0.40455													
11	27.7	27.5	12.8	0.40455													
11	27.7	27.5	12.9	0.40455													
12	27.7	27.5	14.3	0.40456													
12	27.7	27.5	14.5	0.40457													
13	27.7	27.5	16.0	0.40458													
13	27.7	27.5	16.3	0.40459													
14	27.7	27.5	18.0	0.40461													

Figure 107. Mallows' Cp

The subset model with the lowest Mallows's Cp includes: eGamma, hRad,hGamma, iAnimals, iRad, iGamma, iBio, iChem, cGamma, iRdmPrc, ATS, eScanPrc. Therefore the model would be

$$\ln\left(\frac{\pi_i}{1 - \pi_i}\right) = \beta_0 + \beta_{eg}x_{eg} + \beta_{hr}x_{hr} + \beta_{hg}x_{hg} + \beta_{ia}x_{ia} + \beta_{ir}x_{ir} + \beta_{ib}x_{ib} + \beta_{ic}x_{ic} + \beta_{ig}x_{ig} + \beta_{cg}x_{cg} + \beta_{ats}x_{ats} + \beta_{esp}x_{esp} + \beta_{irs}x_{irs}$$

The output data in Figure 108 shows that the model is a good fit and that all of the regressors that are left in the model are significant in determining whether or not a container is detected or not detected with the exception of iRdmPrc. The random percentage of containers selected for intrusive inspection is a regressor that the SSTG chose to leave in the model to be able to predict how the Probability of detecting a dirty container would change based upon the percentage of containers that were randomly selected for inspection.

Binary Logistic Regression: Detected versus eGamma, hRad, ...

Link Function: Logit

Response Information

Variable	Value	Count	
Detected	1	5105	(Event)
	0	2682	
Total		7787	

Logistic Regression Table

Predictor	Coef	SE Coef	Z	P	Odds Ratio	95% CI	
Constant	-2.97964	0.132867	-22.43	0.000			
eGamma	0.215092	0.0629802	3.42	0.001	1.24	1.10	1.40
hRad	0.280516	0.0604222	4.64	0.000	1.32	1.18	1.49
hGamma	1.23749	0.0606417	20.41	0.000	3.45	3.06	3.88
iAnimals	1.28834	0.0619840	20.79	0.000	3.63	3.21	4.10
iRad	0.466768	0.0574378	8.13	0.000	1.59	1.43	1.78
iGamma	1.58231	0.0616637	25.66	0.000	4.87	4.31	5.49
iBio	0.399751	0.0587772	6.80	0.000	1.49	1.33	1.67
iChem	0.308614	0.0597397	5.17	0.000	1.36	1.21	1.53
cGamma	1.92586	0.0653787	29.46	0.000	6.86	6.04	7.80
ATS	-0.0910465	0.0408770	-2.23	0.026	0.91	0.84	0.99
eScanPrc	0.200392	0.0909223	2.20	0.028	1.22	1.02	1.46
iRdmSelPrc	-0.0583792	1.00131	-0.06	0.954	0.94	0.13	6.71

Log-Likelihood = -3757.835

Test that all slopes are zero: G = 2512.801, DF = 12, P-Value = 0.000

Goodness-of-Fit Tests

Method	Chi-Square	DF	P
Pearson	752.201	52	0.000
Deviance	740.532	52	0.000
Hosmer-Lemeshow	133.578	8	0.000
Brown:			
General Alternative	7.035	2	0.030
Symmetric Alternative	5.117	1	0.024

Measures of Association:

(Between the Response Variable and Predicted Probabilities)

Pairs	Number	Percent	Summary Measures	
Concordant	11134071	81.3	Somers' D	0.64
Discordant	2348773	17.2	Goodman-Kruskal Gamma	0.65
Ties	208766	1.5	Kendall's Tau-a	0.29
Total	13691610	100.0		

Figure 108. Minitab Results of New Model

The generated interval plot with a 95 percent Confidence Interval (Figure 109) shows that the active scanning machines like the X-Ray, Neutron, and Gamma Scanners can contribute significantly to the overall probability of detection. Notice from the chart that when an active scanner was present in the system the probability of detection was significantly higher than when the scanner was not in the system. The only exception from this result was the active scanner located at the port of entry where the containers were scanned as they arrive by truck. This was in large part due to the

construction of our model where the model was patterned after a port that had 95 percent of its shipping volume arriving by transshipment, meaning that the majority of the cargo never passed through the port of entry scanner. Out of the 12 dirty containers that arrived that could contribute to the overall probability of detection, only two of the containers were admitted to the port through trucks, thereby limiting the overall effect that the entry scanner could have on the overall probability of detection.

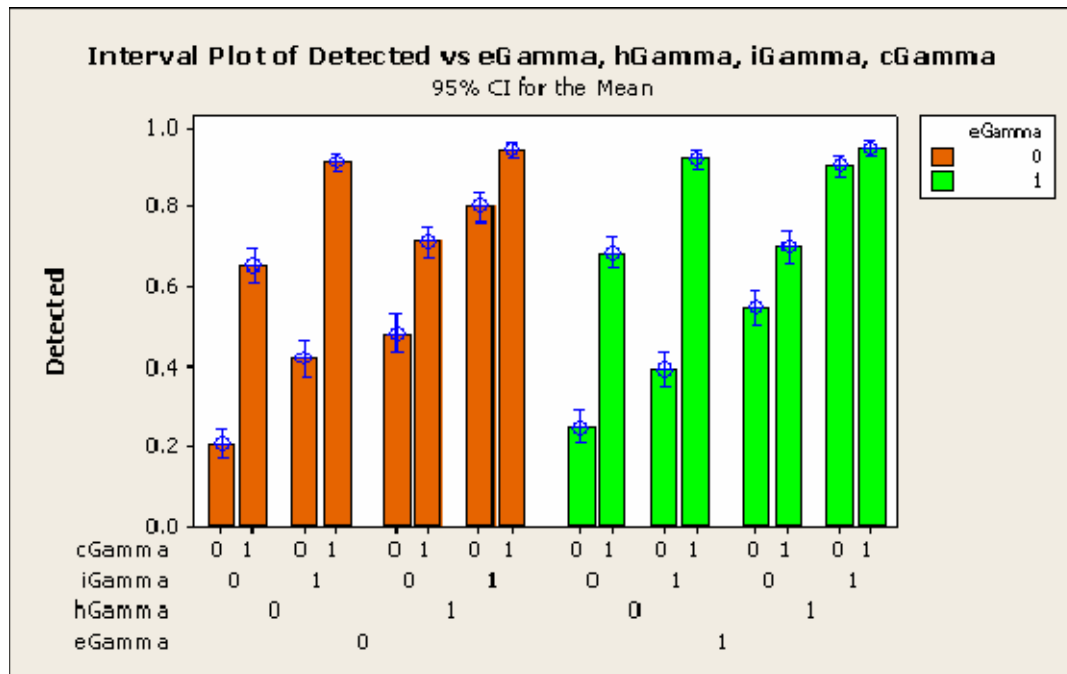


Figure 109. Interval Plots for Gamma Detectors

A comparison of the inspection station sensors interval plots (Figure 110) shows that the chemical sensor did not contribute much to the probability of detection compared to the other sensors located at the station. This could be due to a variety of factors, including the fact that the chemical detector is specifically designed to only detect the presence of certain chemicals and if there are chemicals loaded on the container for which the chemical detector is not designed to detect then the chemical detector would not contribute to the overall probability of detection.

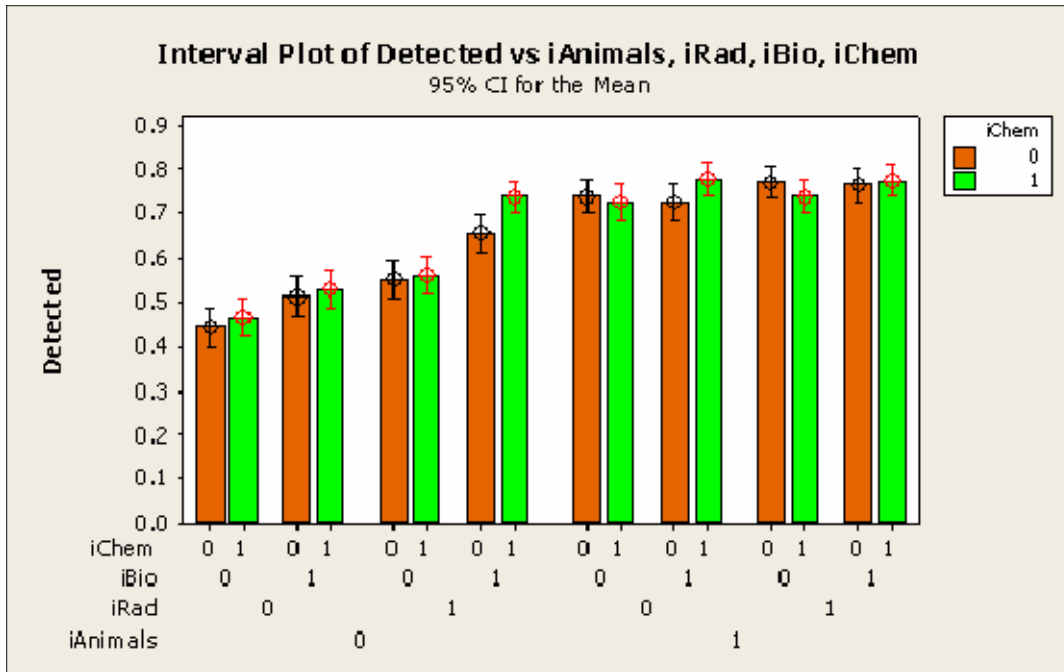


Figure 110. Interval Plot of Inspection Station Sensors

The following interval plot (Figure 111) compares ATS and the entry scanning percentage as a function of probability of detection. It is interesting to note that for ATS level 1 the probability of detection decreases at a port entry scanning percentages of 50 and 100 percent. Both ATS and entry scanning percentage were determined to be non significant in determining the probability of detection in the presence of the other regressor.

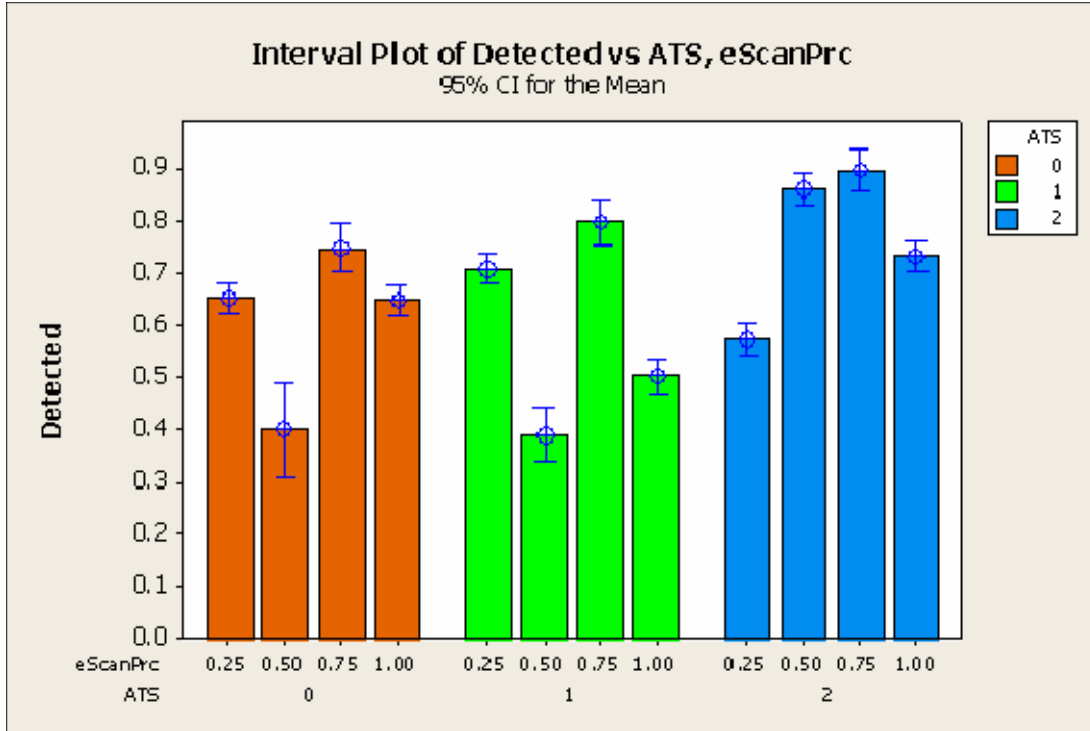


Figure 111. Interval Plot of eScanPrc and ATS

b. Partitioning Analysis

In this section, partition trees were used to interpret the simulation results of different sensor configurations. Partitioning is a data-mining technique especially suited to handle large problems and good for exploring relationships without requiring a good prior model. The findings of partitioning are presented as partition trees, which are intuitive to interpret and understand.

For our model, four partition trees were generated to investigate how the experiment settings of sensor configuration affect the MOP of Probability of Detection (Pd), False Alarm Rate (FAR) and Productivity. Each partition tree comprises a series of splits that are formed by exploring all possible partitions of the data to find the most significant factor that will impact the MOP most at each node of the tree. Hence, each tree enables a quick and statistically powerful diagnosis of the operation boundaries that are most and least favorable to optimizing the MOP under study.

In the following discussion, the partition trees will be interpreted to optimize the MOP of interest; hence they could be traversed from left to right or vice

versa with no fixed direction. The rule of thumb is to interpret the best sensor mix. The direction of description will be included in the figure caption so that the reader can follow the discussion.

As the analysis progressed, trade-offs between system objectives would surface and call for user inputs to influence the splitting of the partition tree. The branching of partition trees can be automatic or by choice. Automatic branching is done by the program and it selects the most significant factor to split branches. Choice branching is done by the analyst to fit real world choices, not unlike our choice to retain the counter-option of deploying the gamma detector that will increase FAR. In this section, the analysis will be mostly automatic to find the most significant factors. In reality, the same partition tree model could be repartitioned using an existing sensor configuration if there are certain features that must be in the system. Such a partition would provide different bounds on the average MOP and would aid the systems engineer in predicting the performance bounds of the configuration under study.

Partition for Probability of Protection

Probability of detection would probably be the most heavily weighted MOP for a stakeholder from the security department. Thus the above partition tree is of utmost interest to find the sensor mix for ensuring high Pd. It should be noted that the partitioning results only optimize one MOP at a time without consideration for tradeoffs with other MOPs. The proposed sensor mix for maximum Pd may or may not conflict with alternative sensor mix to optimize other MOP of interest. Figure 112 shows the partition tree for Pd.

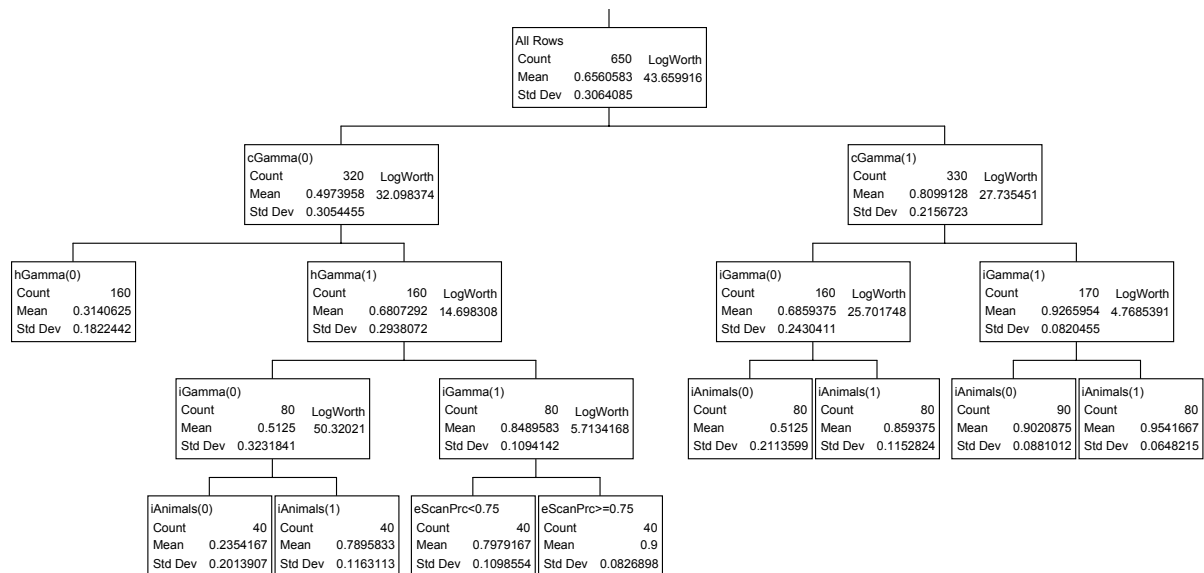


Figure 112. Partition Tree for Probability of Detection (Max Pd, rightmost)

From the topmost of the partition tree, the average Pd for all sensor configurations was 66 percent. At the first split, the most significant factor to influence the average Pd was the presence of a gamma detector mounted on cranes (cGamma). This result was intuitive as the gamma detector scans all cargo while loading them onto the vessel. The difference in deploying a crane gamma detector was an average Pd of 50 percent (without) versus 81 percent (with).

The next best sensor to supplement a crane sensor was another gamma detector at the intrusive inspection team (iGamma), which increased average Pd to 93 percent. Beyond that, stationing animals with the intrusive inspection team (iAnimals) could swing the Pd to 90 percent (without) versus 95 percent with animals. However, the standard deviation of the experimental results did not suggest statistical significance in Pd due to the use of trained animals and therefore it will not be recommended. Conversely, if there was no detector at the intrusive inspection team, the average Pd decreased to 69 percent and could be significantly boosted to 86 percent by deploying trained animals at the intrusive inspection team.

All is not lost without deploying a crane gamma detector. Deploying gamma detectors on mobile scanning units in the holding area (hGamma) could still maintain an average Pd of 68 percent, which is boosted to 85 percent when supplemented

with gamma detectors at the intrusive inspection teams, or boosted to 90 percent when we ensure that more than 75 percent of all incoming land containers were scanned at the fixed point of entry (eScanPrc).

Given that a huge volume of the container traffic was transshipment containers, SSTG expected to find that not deploying gamma detectors in both the crane spreader and holding area would result in an average Pd of 31 percent.

The Pd partition tree showed that deploying gamma detectors is vital in ensuring high Pd. The best locations in descending order were on the crane (81 percent), holding area and intrusive inspection team. Trained animals helped optimize the Pd given their versatility in detecting various materials. With gamma detectors, average Pds of above 90 percent could be achieved. If gamma sensors were not deployed within the sensor configuration, average Pd could be as low as 31 percent.

Partition for False Alarm Rate

The model counted clean, legitimate containers wrongly detained as false alarms. In reality, it is common practice for the port to pass on the cost of inspections and/or detainment to the customers (shipper) who would certainly be extremely displeased. As such, false alarm of the entire port inspection process was a vital statistic that translated to lost productivity, lost goodwill and reputation of the port. Ideally, FAR should be minimized and as such the partition tree would be traversed left to right. Figure 113 shows the partition tree for FAR.

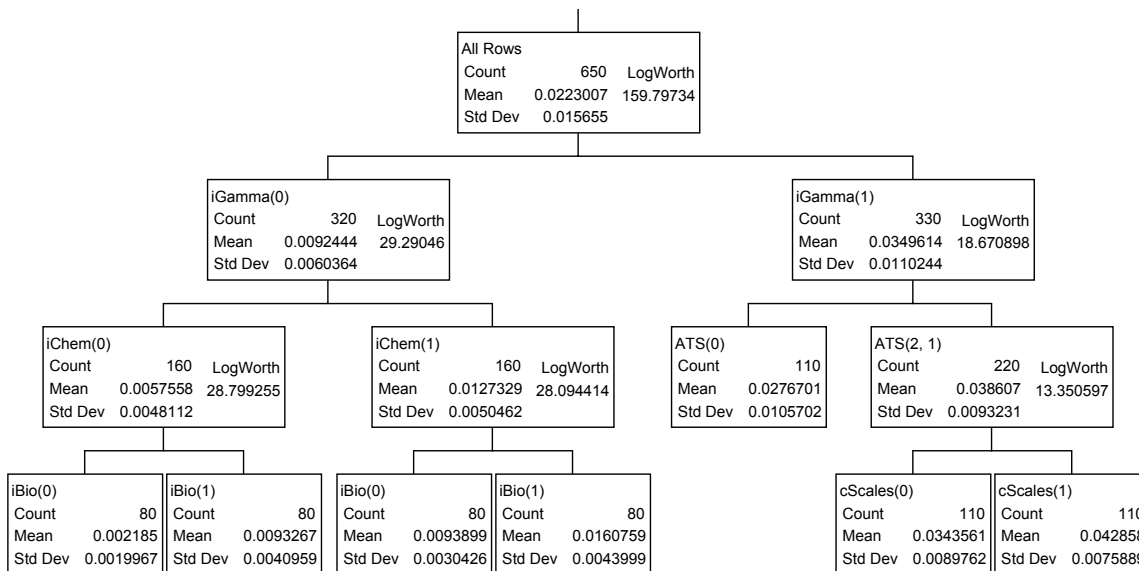


Figure 113. Partition Tree for False Alarm Rate (Min FAR, leftmost)

From the topmost of the partition tree, the average FAR for all sensor configurations was 2.23 percent. At the first split, the most significant factor to influence the average FAR was the presence of a gamma detector with the intrusive inspection team (iGamma). The difference in deploying this gamma detector was an average FAR of 0.92 percent (without) versus 3.50 percent (with). In addition, not having biological or chemical detectors at the intrusive inspection teams would help stabilize the average FAR to 0.22 percent.

As we saw in the Pd partition tree, deploying the gamma detector with the intrusive inspection team helped achieve a high Pd. Hence we may be inclined to tolerate the associated FAR without compromising Pd. Given that the gamma detector was deployed at the intrusive inspection team, the next best way was to not introduce ATS profiling in the sensor system as it would tag more containers for inspection. The resultant FAR would be an average of 2.77 percent (without ATS) versus 3.86 percent (with ATS).

The FAR partition tree showed that deploying the gamma detector with the intrusive inspection team was the main culprit for hiking up the FAR to an average of 3.50 percent. In our early Pd partition analysis, the gamma detector at various locations

had been singled out as significant for ensuring a high Pd. If Pd is valued as more critical than FAR, the FAR associated with the gamma detector has to be tolerated so as not to compromise Pd. Given the deployment of the gamma detector, the average FAR can be capped to 2.77 percent by not introducing additional container inspection volume from ATS risk profiling.

Partition for Productivity

Inspections decrease productivity and hence, the analysis was expected to yield recommendations to not install various sensors. Such findings will be weighed against earlier findings of Pd and FAR optimization and recommended accordingly. Figure 114 shows the partition tree for productivity.

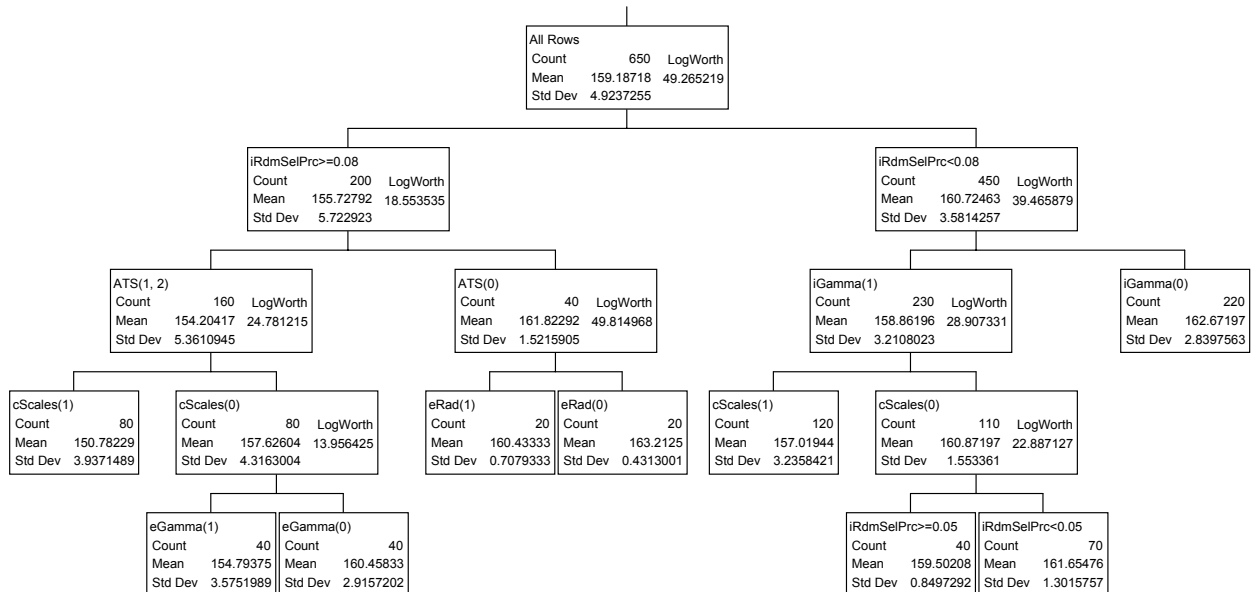


Figure 114. Partition Tree for Productivity (Max Productivity, rightmost)

The simulation was conducted given ample inspection resources, so as not to halt productivity. Hence, SSTG saw only a slight spread of productivity figures of approximately 8 percent about the average. The overall average productivity was 159 containers (loaded) per hour.

The most significant factor that affects productivity was the percentage of total container traffic randomly selected for inspection (iRdmSelPrc). The difference in productivity due to the random selection percentage was 156 containers per hour (more than 8 percent) versus 161 containers per hour (less than 8 percent).

The best productivity of 163 containers per hour was achieved if the random selection was kept below 8 percent and the gamma detector was not deployed at the intrusive inspection team. However, the latter was part of the optimal sensor mix and hence had to be worked around.

Working around the deployment of the gamma detector, SSTG chose not to deploy weighing scales on cranes, as they decrease productivity to 157 containers per hour and has not been shown to be a significant factor in optimizing Pd. Such a configuration achieved an average productivity of 161 containers per hour.

The least favorable configuration comprises random selection above 8 percent, ATS profiling and deploying weighing scales on crane spreaders. Such a configuration brings productivity down to 151 containers per hour.

Both random selection for inspection and ATS risk-profiling proved to be the most significant counter-productivity factors. On the other hand, to optimize productivity, the random selection percentage should be capped below 8 percent. The gamma detector with the intrusive inspection team had resurfaced as a counter-productivity factor but it would not be scrapped as it would compromise Pd. Even with the gamma detector in the system, productivity could still be kept relatively high by not having crane scales in the same system. Additional partitioning suggested further reducing the random selection percentage to 5 percent but the difference is not significant for us to recommend that.

Partition for Inspection Time per Container

As with the productivity analysis, the “average time per container” analysis was expected to yield recommendations to not install various sensors. Such findings would be weighed against earlier findings of Pd and FAR optimization and

recommended accordingly. Figure 115 shows the partition tree for the average inspection time per container.

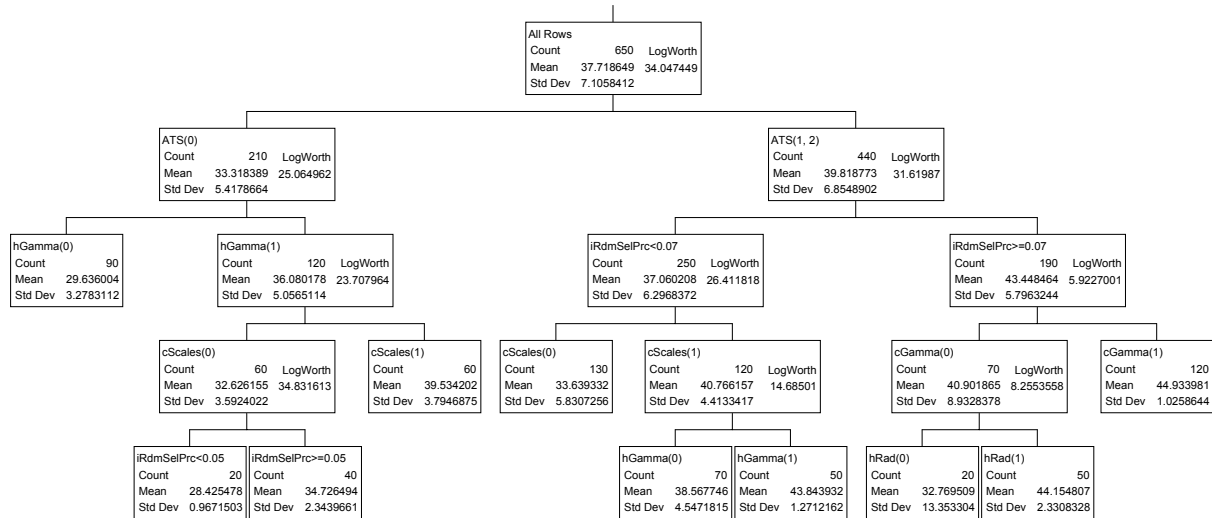


Figure 115. Partition Tree for Inspection Time per Container (Min Time, leftmost)

The average inspection time per container was 37.7 minutes, with a standard deviation of 7 minutes. This MOP was most significantly affected by the presence of ATS risk-profiling, which affects all containers. The difference in average inspection time was 33.3 minutes (without ATS) and 39.8 minutes (with ATS). If there was no ATS risk profiling and no gamma detector in the holding area, the average inspection time per container was further reduced to 29.6 minutes.

The SSTG reserves the need to deploy the gamma detector and thus would have to face an average inspection time of 36.1 minutes. If the gamma detector was deployed, the crane scales detector should not be deployed as it would further increase inspection time.

The least favorable configuration comprised ATS risk profiling and random selection percentage. This finding coincided with the productivity analysis finding. Both processes combined raised the average inspection time per container to 43.3 minutes.

The best configuration to optimize average inspection time per container (with consideration for Pd) was to remove ATS risk profiling, deploy the gamma

detectors in the holding area and not to deploy crane weighing scales. Such a configuration would bring the average inspection time per container approximately 32.6 minutes.

Both random selection for inspection and ATS risk-profiling proved to be the most significant factors and should be avoided if we want to minimize average inspection time per container. Otherwise the resultant average inspection time per container could be as high as 44.9 percent.

Partitioning Analysis Conclusions

The individual partition analysis on the MOPs had enabled appreciation of the significant factors driving each MOP. The final conclusion was based on trade-offs between these factors and the (qualitative) weight of the MOPs. The probability of detection remains the ultimate objective and thus the optimum sensor configuration must deploy gamma detectors in one or more of these locations (descending preference) on the crane, on mobile inspection teams in the holding area and/or at the intrusive inspection teams. Trained animals complement the inspection efforts too. Overall such a combination could achieve average probability of detection of above 90 percent.

However, the use of gamma detectors would compromise the other MOP of FAR, productivity and average inspection time per container. Nonetheless Pd was valued more importantly and hence subsequent recommendations would work around the fact that gamma detectors would be deployed.

Additional recommendations include: removing ATS risk profiling, limiting random selection to less than 8 percent of total container volume and not deploying crane scales. These factors will help achieve average FAR of 2.77 percent, average productivity of 161 containers per hour and average inspection time per container of 32.6 minutes

c. Data Analysis Conclusions

The analysis of the model raw output data has helped the SSTG to determine which of the sensors are significant in changing the values of our response variable or MOPs. Through linear regression and partition analysis, the SSTG have

learned that for the specific port modeled; with a high transshipment volume; to have a high probability of detection, gamma scanners at the inspection station and also at the crane spreaders was needed. Both the linear regression analysis and the partition analysis provided consistent answers to the factors that were important in the probability of detection. The single most important piece of equipment that provided the largest increase in probability of detection was due to the gamma scanners and it is essential to place them in locations where the largest portion of the containers will be scanned by the equipment. In addition, a well equipped, efficient, inspection team cadre that can keep up with the sheer volume of containers that need to be inspected due to false alarms and random selection is essential in providing the highest probability of detection. Minimizing false alarms by reducing the number of randomly selected containers and also by reducing the ATS level to 0 ensured that the number of containers that have to go to the inspection station for an intrusive search would be minimal. The linear regression model showed that the random selection percentage and the ATS level were insignificant in the detection or non-detection of dirty containers, and therefore there is only a slight penalty in probability of detection. This seems counter intuitive and highlights an area of concern about the model assumptions. In order for the model to process all of the dirty containers in the 12 hour simulated run time, the number of inspection teams and the efficiency with which those teams processed containers were increased. This helped to ensure that enough of the dirty containers had been processed through the system to get credible probability of detection. In reality, there would be a higher penalty in probability of detection and lost productivity with inspection teams that took longer to process containers compounded with fewer teams. When the model was first run with five inspection teams that could process the containers in a one hour timeframe, the number of processed dirty containers were very few due to the very long queues at the inspection stations. This would have created a much larger penalty for productivity and container throughput would have also declined. The important result is that even for highly accurate sensors with low false alarm rates the number of containers that need to be inspected can be overburdening on the port facility. This problem is compounded by additional sensors.

5. Cost Estimation

In developing the cost analysis, the system life cycle cost was considered and that includes the research and development phase, the production and implementation phase, the operation and support phase, and the disposal phase. As all of the products considered in the SSTG alternatives generation are already developed by private companies, the research and development cost is not included in the estimation. Additionally, the disposal cost for the system is also excluded from the estimation. As such, the individual cost for the production, implementation, operation, and support for each system element and component of the various alternatives were aggregated to derive the total system cost for each alternative.

The system is expected to be fully implemented and inclusive of operation for 20 years. Each system component and element will have its unique life cycle cost and maintenance schedule. After 20 years, the system is expected to be upgraded or replaced with more advanced technologies and future daily operational cost is likely to be lower.

Each system component and element unit cost were estimated and then multiplied by the actual units of the component and element to derive the sub-system cost. Each reference cost is normalized to US 2007 dollars. Future inflation is not considered in the system life cycle cost.

a. Manifest Screening

The Government so far had spent 34 million dollars over six years on developing the Automated Targeting System (ATS). The additional maintenance and operational cost was estimated to be 6.7 million per year. Most of the maintenance and operation cost involves paying the large number of operators necessary to handle the volume of manifests each day.

The cost to improve the current ATS to ATS+ was estimated to be at 10.5 million 2001 dollars per year. Table 61 shows the breakdown for developing ATS+. Normalized to 2007 dollars, the cost is estimated to be 12.2 million dollars. Majority of the cost components were due to the production support and maintenance changes with little over half the cost per year. The estimated costs were developed before the ATS was

fully developed. While the current estimate is likely to differ, the group continues to use the older estimates due to lack of references. It was assumed that there was no cost associated to the source port for not implementing manifest screening.

Production Support & Maintenance Changes	\$ 5,500,000
Software Testing	\$ 800,000
Travel, Supplies, Training, Equipment, Licenses	\$ 200,000
Infrastructure Upgrades	\$ 300,000
1. TOTAL MAINTENANCE	\$ 6,800,000
Analysis, Design & Coding/Enhancements	\$ 2,500,000
Software Testing	\$ 800,000
Travel, Supplies, Training, Equipment, Licenses	\$ 100,000
Infrastructure Upgrades	\$ 300,000
2. TOTAL ENHANCEMENTS	\$ 3,700,000
TOTAL Maintenance & Enhancements	\$10,500,000

Table 61. Cost of Improving the ATS System in 2001 Dollars

b. Scanning Location

Each of these units employs X-ray and Gamma ray scanners as well as radiation detectors. For this reason, SSTG included the cost of these scanners in the cost of each screening location.

The ROM (Rough Order of Magnitude) cost of the mobile scanning system is not available in the public domain. As such, SSTG estimated the cost by

decomposing the system into various component and search for the retail price of each components, parts and elements. A large truck for housing the equipment and transport the equipment to scan the container is estimated to cost between 60 thousand to 150 thousand dollars. The primarily cost driver for the truck is the size and horsepower. 150 thousand dollars will be used as the estimate cost due to the fact that the truck will have to be customized to house the x-ray and gamma ray scanners. In addition, the annual maintenance costs, gas cost and operator cost were separately estimated. The average trucker salary is 50,000 dollars. The average maintenance costs for the truck is 3,000 dollars. Gas usage is harder to estimate because the truck will only move around the confines of the port and with the availability of additional mobile scanning systems, each truck is expected to travel less mileage. The estimation is simplified by assuming one mobile system will be used for the entire port. Referencing the map of Port of Oakland, the end to end distance is approximately 4 miles across. Figuring that the truck will make 1 round trip an hour, the truck will roughly travel 32 miles a day. In a year, the truck is expected to travel 11,200 miles. The national average diesel cost per gallon is 2.792 dollars. The average truck gets roughly 10 miles per gallon when fully loaded and that translate for the truck annual gas cost to approximately 3,200 dollars.

According to the Financial Times, each X-ray machines for inspecting cargo containers cost 2.2 million dollars. The radiation detector cost roughly 337,000 dollars a piece according to the U.S. General Accounting Office. The operator paycheck, regular maintenance and electricity cost summed up to 183,000 dollars a year for the operational and support. The total life cycle cost for the mobile scanning system is 5.96 million dollars. Table 62 shows the breakdown of the costs estimation for the mobile scanning system.

Mobile Scanner	Initial Cost	Life Cycle(yrs)	Maintenance Cost (Per yr)	operator cost (per yr)	electricity/gas etc (for 20 yrs)	Total!!!! (over 20 yrs)
Truck cab and Chasis	\$150,000.00	20	\$3,000.00	\$50,000.00	\$3,200.00	\$6,484,000.00
X-ray equipment	\$2,273,000.00	20	\$5,000.00	\$60,000.00		
Radiation detection equipr	\$337,000.00	20	\$5,000.00	\$60,000.00		

Table 62. Cost Estimation for Mobile Scanning System

The X-ray Fixed Entry Systems cost 3.7 million dollars in 1996 according to the United States General Accounting Office. Adjusting for inflation to 2007 dollars, a fixed X-ray system would be 4.74 million dollars. The United States General Accounting Office estimated that the maintenance, operator and electric costs would run up to 2.1 million dollars a year. Multiplying by 20 years gives a whopping 42 million dollars over the lifespan of the fixed scanner system, putting the total cost at 46.7 million dollars. Table 63 shows cost breakdown of the fixed scanning system.

Fixed Entry Scanner	Initial Cost	Life Cycle(yrs)	Maintenance Cost (Per yr)	operator cost (per yr)	electricity/gas etc (for 20 yrs)	Total!!!! (over 20 yrs)
X-ray sytem	\$4,740,000.00	20			\$2,100,000.00	\$46,740,000.00

Table 63. Cost Estimation for Fixed Scanning System

According to the Port of Auckland's website, crane spreaders cost roughly 6.5 million U.S. dollars. The cost varies on size, type and manufacturer. Including the sensor package at an approximately one million dollars, the total acquisition is estimated at 7.5 million dollars. Due to high strain and impact vibration caused by the act of loading and unloading the containers, replacement parts and maintenance costs are estimated at 600,000 dollars. The operator paycheck and the electricity usage add another 60,000 dollars to the operational cost annually. Each crane spreader scanning system life cycle cost is approximately 20.7 million dollars. Table 64 shows the cost breakdown for the crane spreader scanning system.

Crane Loading Spreader	Initial Cost	Life Cycle(yrs)	Maintenance Cost (Per yr)	operator cost (per yr)	electricity/gas etc (for 20 yrs)	Total!!!! (over 20 yrs)
Crane Loaders	\$6,500,000.00	20	\$100,000.00	\$50,000.00	\$10,000.00	\$20,700,000.00
Sensor Package	\$1,000,000.00	20	\$500,000.00			
	\$7,500,000.00					

Table 64. Cost Estimation for Crane Spreader Scanning System

c. Non-Intrusive Container Screening

Like guide dogs, drug and bomb sniffing dogs require lots of training and care costs. A guide dog team (dog and handler) costs \$40,000 to train, and a detection dog can expected to be comparable [61]. The average work span for these dogs ranges from six to eight years [62]. The cost for dogs and training, as well as for the annual care, maintenance and handling are provided in the table below. The 20 year total cost

provides for three replacement dogs and their training, as the dogs retire to safe and happy homes after their service. Table 65 shows the cost breakdown for trained animals.

Trained Animals	Initial Cost	Life Cycle(yrs)	Maintenance Cost (Per yr)	operator cost (per yr)	electricity/gas etc (for 20 yrs)	Total!!!! (over 20 yrs)
Dog from breeder	1000	6 to 8				3000
Training	40000					120000
Shelter / Play Area	1000		100			3000
Food			500			10000
Veterinary Care			200			4000
Grooming			100			2000
Operator Cost (40 hr work week for 50 weeks)				62000		1240000
Misc (collars/beds...)			100			2000
					TOTAL (per unit for 20 yrs)	1384000

Table 65. Cost Estimation for Trained Animals

Truck scales are easily available and have become very durable through continued technology advances. A truck scale including equipment, foundation, freight, installation, and startup has an estimated cost of between \$60,000 and \$70,000 [63]. It is expected to last 15-20 years, in high traffic, with proper maintenance. This maintenance included semi-annual inspections for the first five years and quarterly inspections every year thereafter. Table 66 shows the cost breakdown for scale.

Scales	Initial Cost	Life Cycle(yrs)	Maintenance Cost (Per yr)	operator cost (per yr)	electricity/gas etc (for 20 yrs)	Total!!!! (over 20 yrs)
Initial costs	70000	20				70000
Inspections (1st 5 years)			400			8000
Inspections (Quarterly after 1st 5 yrs)			800			16000
Operator Cost (40 hr work week for 50 weeks)				62000		1240000
Electricity					minimal	
					TOTAL (per unit for 20 yrs)	1334000

Table 66. Cost Estimation for Scales

d. Intrusive Container Screening

Portable radiation detectors are available commercially for as little as \$400 a piece [64]; however, Lawrence Livermore National Laboratory estimates the cost to be closer to \$2000 each [65]. With two detectors required for each person, to ensure they always have one available in good working order for each shift, these still are relatively inexpensive to implement. Additionally, almost no maintenance is required although their small size will make them prone to loss as well as dropping and cracking. Table 67 shows the cost breakdown for the portable radiation detector.

Portable Radiation Detectors	Initial Cost	Life Cycle(yrs)	Maintenance Cost (Per yr)	operator cost (per yr)	electricity/gas etc (for 20 yrs)	Total!!!! (over 20 yrs)
Initial Costs (2 units)	1000	10				4000
Replacement (new unit every 4 years)	1000					5000
Operator Cost				62000		1240000
					TOTAL (per unit for 20 yrs)	1249000

Table 67. Cost Estimation for Portable Radiation Detector

A human inspection team for intrusive inspections of suspicious containers is provided for by U.S. Customs and not incurred on the ports or shipping companies. However, a cost will incur by the U.S. Government. The inspection teams usually are manned by five personnel. Each personnel are expected to receive equipment, training and other supplies to carry out their tasks. The estimated cost for equipment is 100 thousand dollars for hand held radiation detectors, chemical scanners and biological screeners. Training is roughly another two thousand dollars for scenario mock up equipment, instructor and trainee pay. The expected maintenance cost for the equipment is 250 dollars per year and the salary of each member is on average 50 thousand dollars. Multiplying for a life-cycle of 20 years and adding the different parts of the system, the total lifespan cost comes to be about 5.6 million dollars. Table 68 shows the cost breakdown for employing the customs inspector and equipped with the necessary equipment.

Human Inspection Team	Initial Cost	Life Cycle(yrs)	Maintenance Cost (Per yr)	operator cost (per yr)	electricity/gas etc (for 20 yrs)	Total!!!! (over 20 yrs)
1 Worker	\$2,000.00	20	\$55,000.00	5		\$5,615,000.00
Equipment	\$100,000.00	20	\$250.00			

Table 68. Cost Estimation for Customs Inspector

Remotely Operated Robots are used everyday in the military and by the police force as bomb disposal units. These robots would be easily reconfigured with a sensor package to do inspections of cargo containers for undesired cargo. According to one of the leading manufacturer's website, Security Pro USA, the cost for a robot system is 26 thousand dollars. The cost for an x-ray onboard is an additional 3 thousand dollars. The cost for a complete weapons of mass destruction sensor package (biological, radiological and chemical) is 24 thousand dollars. Maintenance and operating cost figures would be around 100 thousand dollars per year considering parts and labor costs for maintenance and paying two operators, one to operate the robot and one to operate the

sensor packages. The total cost comes to a little over two million dollars for the lifespan. Table 69 shows the cost breakdown for remotely operated inspection robots.

Robot Inspection Units	Initial Cost	Life Cycle(yrs)	Maintenance Cost (Per yr)	operator cost (per yr)	electricity/gas etc (for 20 yrs)	Total!!!! (over 20 yrs)
Robot Cost	\$26,000.00	20	\$1,000.00	\$45,000.00		\$2,011,597.00
Xray Machine	\$3,081.00	20	\$500.00	\$50,000.00		
WMD sensor package	\$22,516.00	20	\$1,500.00			

Table 69. Cost Estimation for remotely Operated Inspection Robots

e. Smart Tags

RFID (Radio-Frequency Identification) technology is becoming more and more prevalent today as major corporations and military departments have started to use this method to track goods and streamline the supply chain [66]. Active tags can cost as little as three dollars apiece and those which are active and also contain GPS and wireless communication capabilities can cost as little as five hundred dollars apiece. Software upgrades and infrastructure systems will cost an additional 200,000 to millions of dollars. These systems will be costly to implement, but could, in the long run, save shipping companies money because they will greatly reduce lost shipments and stolen goods. The exact cost of widespread implementation is uncertain, as these have only been installed on containers in small quantities. As these smart tags will not affect the models created because their capabilities are not relied on for protection until the container is out of the source port and in-transit, the smart tag costs will not affect the cost benefit analysis.

f. Alternative Cost Analysis

The cost of each alternative SSTG presented can be found by summing all of the component costs for each alternative once they have been multiplied by the number of each component. Table 70 shows the number of each system used in developing the alternatives.

Description	Value
Fixed Point of Entry	
Number of servers (lanes) at the point of entry	10
Holding Yard	
Number of servers (mobile non-intrusive scanners) at the holding areas	5
Cranes / Ship Loading Area	
Number of servers (cranes) in port	11
Intrusive Inspection	
Number of servers (inspection teams) for intrusive inspection	7

Table 70. Number of Systems Used in Each Inspection Station

One sees that ten servers were modeled at the point of entry inspection location. However, ten servers would realistically not be installed in all of the alternatives. The status quo alternative only inspects 5 percent of the cargo volume. When 5 percent inspection is done by ten servers, as modeled, the utilization rate for each is very low. The utilization values are shown in Table 71.

#	System					Minimum Units That Must Be Implemented			
		eUtilization	hUtilization	iUtilization	cUtilization	Fixed Entry e(10)	Mobile Units h(5)	Intrusive Inspection Teams i(7)	Cranes c(11)
1	Status Quo	0.01%	0	1	0	1	0	7	0
2	100% Vol Inspection	0.19%	0	0.98814	0.26826	1	0	7	3
3	Improved Loading Search	0.00%	0	1	0.25509	0	0	7	3
4	Min Port Operation Disruption	0.00%	0	0	0.27512	0	0	0	3
5	High Performance	0.00%	0.1746	0.99728	0.2375	0	1	7	3
6	100% Intrusive Inspection	0.00%	0	1	0	0	0	49	0

Table 71. Utilization of Servers at Inspection Stations for Each Alternative

Therefore, for the alternatives cost analysis, the minimum units required to complete each inspection was figured by multiplying the utilization rate by the number of servers modeled to determine how many would be implemented. For example, in the status quo alternative, one fixed entry system is all that would be needed to handle the 5 percent cargo inspection required. With these normalized values, Table 72 shows the cost breakdown and total cost of each proposed alternative.

Alternative	Components	Unit Cost	Units Required	Cost (in US 2007 millions)	Total Alternative Cost (in US 2007 millions)
Status Quo	Fixed entry point	46.74	1	46.74	96.962
	(x-ray)				
	(scales)	1.334	1	1.334	
	Human	5.6	7	39.2	
	Animal	1.384	7	9.688	
100% Volume Inspection	Crane Spreader	20.7	3	62.1	159.062
	(x-ray)				
	(radiation detectors)				
	(scales)				
	Human	5.6	7	39.2	
	Animal	1.384	7	9.688	
	Fixed entry point	46.74	1	46.74	
	(x-ray)				
Improved Loading Search	(scales)	1.334	1	1.334	
	Crane Spreaders	20.7	3	62.1	110.988
	(x-ray)				
	(radiation detectors)				
	(scales)				
	Human	5.6	7	39.2	
	Animal	1.384	7	9.688	
Minimize Port Operations Disruptions	Crane Spreaders	20.7	3	62.1	62.1
	(x-ray)				
	(radiation detectors)				
	(scales)				
High Performance	Mobile System	6.484	1	6.484	82.668
	(x-ray)				
	(radiation detectors)				
	Crane Spreaders	20.7	3	62.1	
	(x-ray)				
	(radiation detectors)				
	(scales)				
	Remotely Operated Inspection	2.012	7	14.084	
	(x-ray)				
	(radiation detectors)				
	(scales)				
100% Intrusive Inspection	Human (includes equipment)	5.6	7	39.2	62.972
	Animal	1.384	7	9.688	
	Remotely Operated Inspection	2.012	7	14.084	

Table 72. Cost Estimation for Six Alternatives

6. Cost Benefit Analysis

To determine the utility for the cost benefit analysis, the results from the model were grouped into a table. The utility functions were designed to translate the raw score for each MOP into utility score. The total utility score for each alternatives were then

computed based on the weight assigned to each MOP. As the stakeholders were not available to participate in a survey to state the preferences of each MOPs, SSTG was unable to use Analytical Hierarchical Process to determine the weight of each MOP. As such, each MOP is assigned the same weight and multiplied with each utility score to derive the total utility score. The weighted utility score for each alternative is shown in Table 73. The High Performance alternative has the highest utility score of 90.57.

High Performance	90.57
Improved Loading Search	87.61
100 % Vol Inspection	88.72
100 % Intrusive Inspection	47.09
Status Quo	59.37
Min Port Operation Disruption	60.64

Table 73. Rank of Alternatives Based on Utility

Figure 116 shows the graph of the utility scores versus the system life cycle cost for the six alternatives. From the cost benefit analysis, two alternatives can be eliminated by inspection. The 100 percent Volume inspection alternative and the Improved Loading Search alternative both have higher costs and lower performance compared to the High Performance alternative and can be eliminated. The 100 percent Intrusive inspection alternative was also eliminated because of the time added per container passing through the model was enormous and economically infeasible for shippers and distributors. The remaining alternatives worth of consideration were Minimum Port Operation and High Performance. While High Performance scored the highest, decision maker will have to decide the need to spend additional US\$20.5 millions to raise the score from 60.64 to 90.57

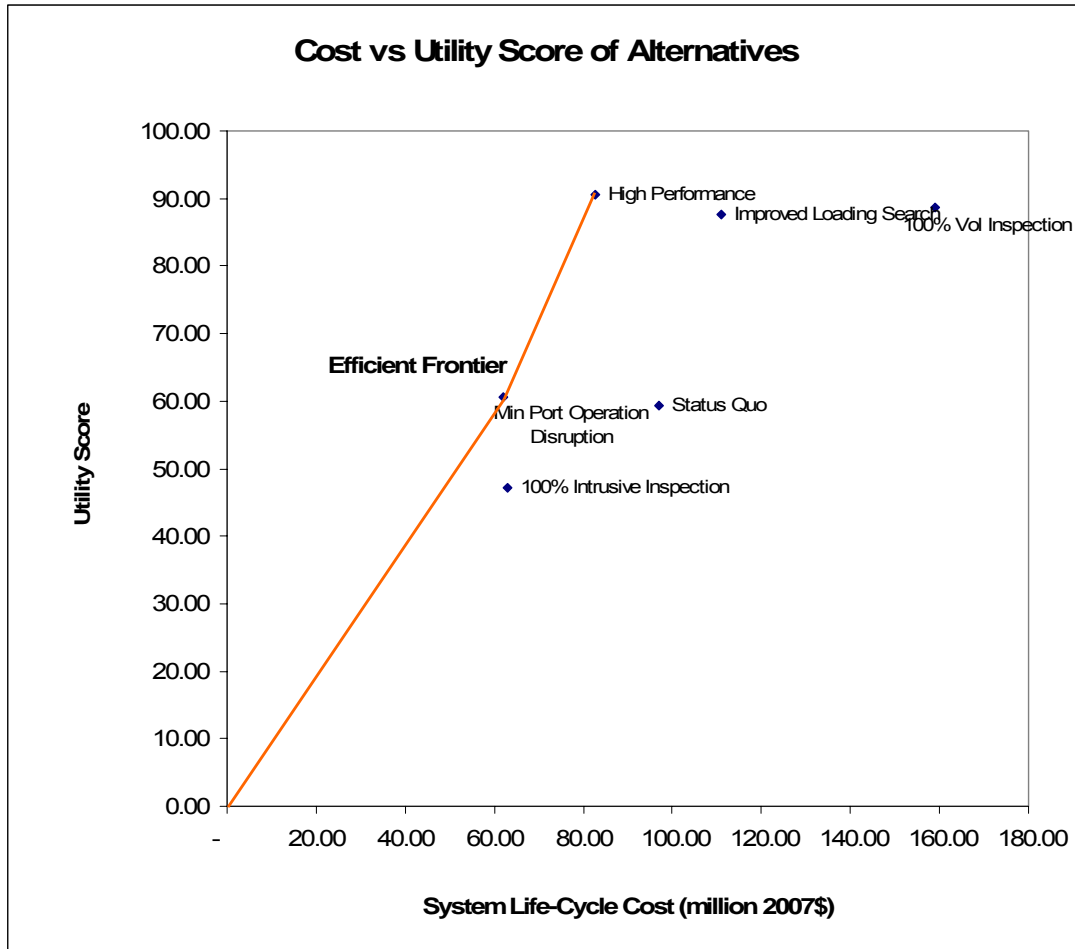


Figure 116. Cost vs Utility Score of Alternatives

V. INTERNAL PERSONNEL THREATS GROUP

A. PROBLEM DEFINITION

1. Needs Analysis

a. System Decomposition

The system decomposition enabled the group to identify a hierarchical structure and the major functions and components of a port internal security system. The three levels of the hierarchical structure were super, lateral, and subsystems. The super systems relative to the port internal security system were national intelligence agencies, state/ federal legislation and the International Maritime Organization. Lateral systems included local police, CBP, USCG and security agencies. Subsystems included biometric readers, sensors (like CCTV), security teams, command centers, communication networks and portable database computers.

The system includes structural, operating, and flow components. The structural components consist of force (including patrol and inspection assets), ISR, Command and Control (C2) Centers (including analysis/response teams), Communications Systems, and decision support. Operating components included sensor networks, Inspection Teams, C2 Centers, Intelligence Centers, and communications networks.

The following are the four categories in enhancing port security undertaken by various agencies in the Port of Singapore with regard to internal personnel.

- Port Compound Security – compartmentalize the port into zone to moderate and monitor cargo and personnel movement.
- Enhanced Port Border Security – undertake measures to protect the perimeter of port compound.
- Cargo Clearance – measures undertaken to pre-verified shipment details and conduct security spot check to detect any illegitimate cargos.
- Personal Clearance – measures undertaken to ensure the legitimacy of workers and crew.

PSA has the sole responsibility of ensuring the security of the port; safeguarding everything in the port premises except immigration and customs issues.

However, security issues that threaten national interest will have close cooperation with the government agencies (e.g. SPF and ICA).

PSA has implemented intelligent security monitoring system on its compound to monitor and detect suspicious activities (e.g. suspicious baggage/items, intrusions to restricted zone, tampering of cargos/containers). Measures also include alarms on restricted access equipment.

Extensive security measures are undertaken to pre-verify shipment and conduct of effective cargo checking. Singapore, being one of the busiest ports in world, poses a great challenge in ensuring the legitimacy of goods. Most importantly, it enables law enforcement the chance to detect materials (or even weapons) that threaten the interest of the nation. Deployed technology equipment such as x-ray scanners, IED scanners, and sniffers further assist the detection capability of law enforcement.

There are two levels of concern in personnel clearance: facility workers and ship's crew. The access control of workers in the compound has to be enforced to prevent any disruptive acts. Internal staff has to execute background checks to ascertain the necessary credibility and trust related to the accessibility of information that may be sensitive and may cause severe consequences with the security of the port.

Authenticity in access control for workers is also enabled through the employment of biometrics. However, such an implementation has tremendous impact to the count in the measurement of efficiency. Therefore, such measures are employed where the threat condition has elevated.

As for the crews, checks and procedures that are similar to immigration enforcement are conducted (e.g. authenticity and validity of passport holders).

b. Stakeholder Analysis

The scope this study involves multiple stakeholders that involve many international agencies, the U.S. Navy, and local port operators with the main purpose of identifying the critical assumptions and constraints of the problem statement. Globalization has created a growth of port related activities that require close cooperation

of ports around the world. Therefore, as part of the integral studies, stakeholders from the Ports of Singapore will also be analyzed.

Basically the team has identified a group of stakeholders and divided the stakeholders into different level based on their hierarchy of roles and responsibilities in shaping the port security as shown in Figure 117.

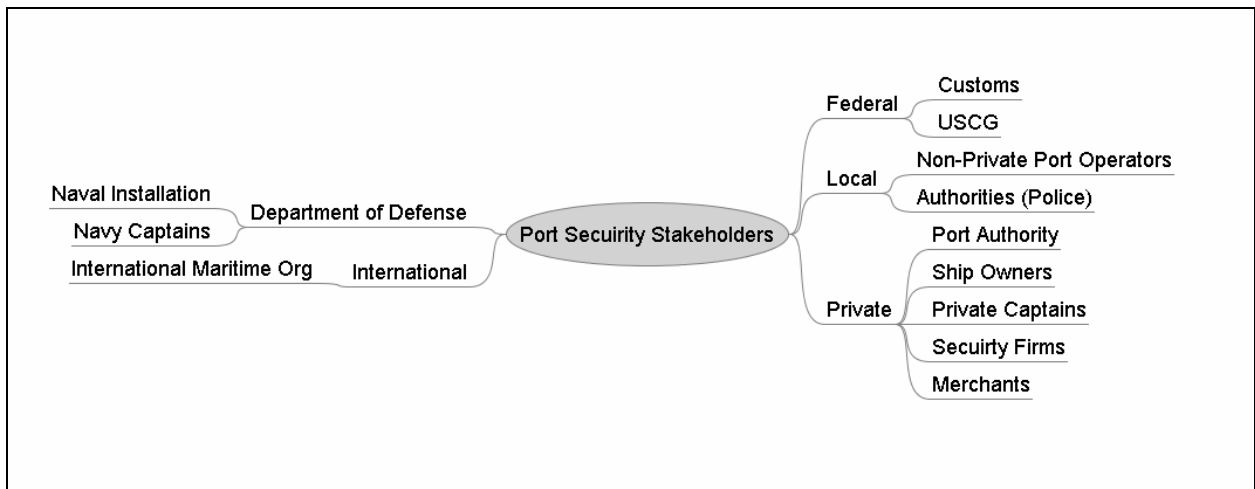


Figure 117. IPTG Stakeholders

The two primary stakeholders that have contributed greatly to shaping our perspective and understanding all the associated issues with port security are: The Port Authority of Oakland, and the Port of Singapore.

On 19 January 2007 the Security director for the Port of Oakland extended an invitation for the PSS12 to directly interview with all the key organizations that contribute to the security operation at the port. In attendance were the Port of Oakland, USCG, and the two terminal operators. The Port of Oakland Authority represented the city of Oakland who owns the port and its infrastructure. The terminals are then leased by the city to the terminal operators. There are 11 terminals in the Port of Oakland, leased to nine different operators servicing over 50 shipping companies. The Port of Oakland is predominantly designated as a container port. The primary focus of the terminal operators are the daily tasks of loading and unloading containers on and off ships in the most cost

efficient manner. The three stakeholders that were present at the meeting came with different perspectives, different priorities and conflicting requirements.

As for port security, the Port of Oakland plays the role of a landlord focused on maintaining a balance between following the security guidelines set by the DHS through the USCG, while ensuring the leasers of the terminals are satisfied with the operating environment. The USCG is the security enforcer who places security guidelines, requirements, and fines upon the port authority and the terminal operators. The port terminal operators were the IPTG's most relevant stakeholders due to their extensive exposure to the inner working of the ports. They are also the primary means for identifying potential security risks.

With this background, there were a few keys take-away from the meeting. In general, all stakeholders agree that the port security has not received adequate attention at the Port of Oakland, and there is definitely room for improvement. All three stakeholders listed various on-going projects that could offer near-term solutions (i.e. Vessel Identification System (VIS), biometric ID cards for the workers, WMD containers scanners). However, as the meeting progressed, there are two statements that seem to perpetuate: 1) there is very limited funds available from any of the three stakeholders. The USCG funding is distributed by the Department of Homeland Security. The terminal operators are effectively working as freelance contractors to the shipping lines, and due to the competitiveness of the shipping business, the margin is small and there are not readily available funds established for security purposes. 2) Commerce is the life blood of the port and cannot be disrupted.

An interview was conducted with officers from the PSA and Maritime Port Authority. It was mentioned that personnel accessibility and cargo is of concern to the security of the port. The newly implemented biometrics access control system is one method to help correct the access control procedure to the port premises. Although current access card control systems are good, surveillance systems must be sensitive enough to detect any illegitimate activities on the ground.

Personnel assigned as staff to the facility would be pre-screened to the necessary clearance level as part of the background check. Policies and procedures would be implemented to safeguard and prevent information deemed useful towards the vulnerability of the system, allowing illegal activity to take place. One constraint is that the full-fledged implementation security measures will be detrimental to port efficiency when security threat heightens.

c. Input-Output Model

The input-output model is helpful to scope and bound the problem. When developing the model, the inputs that are necessary and the outputs that are produced by the system are analyzed. Inputs may be controllable or uncontrollable. Controllable inputs may be further divided into physical, human, informational and economic inputs, while uncontrollable inputs may be further divided into environmental characteristics and existing conditions. These inputs in the system result in intended outputs and by-products as shown in Figure 118.

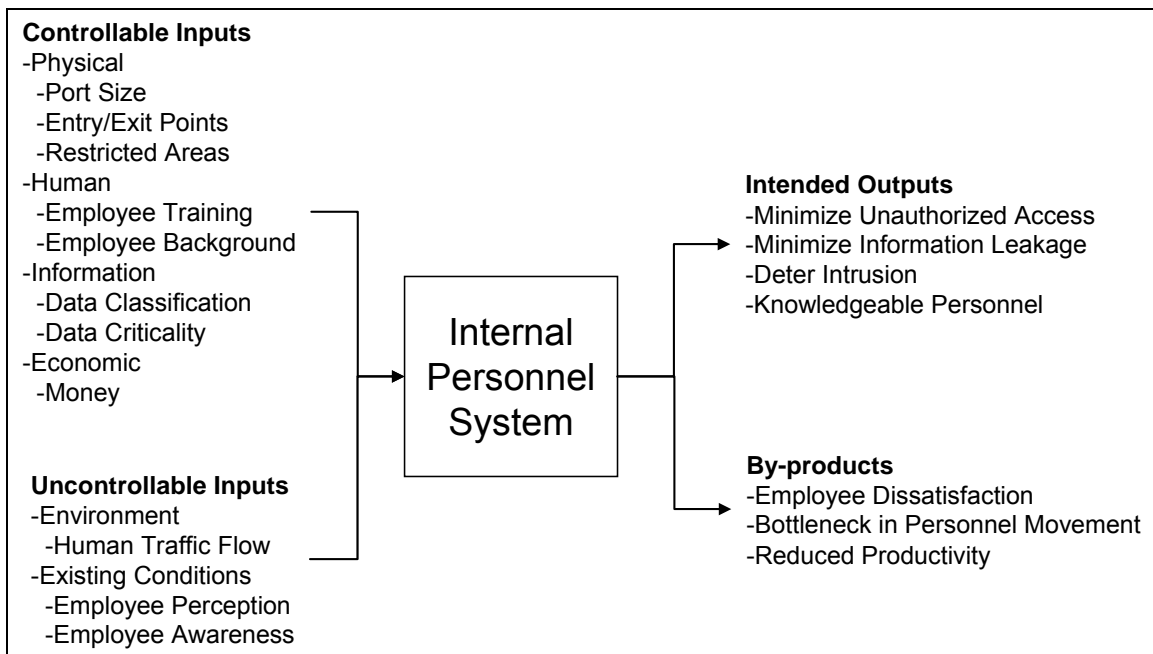


Figure 118. IPTG Input-Output Model

The physical inputs to the system include the physical size of the port, the number of entry and exit points, and the number of restricted areas within the port premises. This is important as there is a need to regulate the flow of personnel in and out of the port, as well as personnel moving within the port. The human inputs include employee training and the background information of the employee. Proper training would ensure the employee is aware of the security implication, their responsibilities, and accountability. The results from the employee background check would translate to the level of security clearance that would be granted. The informational input includes data classification and correspondingly data criticality. It is prudent that the various types of data within the organization be properly identified and classified, enabling data safeguards to be placed to ensure data integrity and availability. Finally, the economic inputs include the amount of money needed to implement the system.

Environmental inputs include the flow of human movement, which is difficult to control, especially during peak hours. Some existing conditions that are inputs to the system are the employee general perception to security measures, as well as their awareness of the security implication of their work. This has impact of the output of the system as a lack of security awareness or a negative perception to security would cause an employee to circumvent the system that is put in place.

The most important outputs that are intended are deterrence to intrusion, minimal unauthorized access, minimal informational leakage, as well as a knowledgeable workforce. Deterrence is one of the goals of the system, when put in place, may cause any potential security intruders to reconsider before acting. If deterrence fails, it is important that any unauthorized access within the port be kept to a minimum, whether intended or unintended, so as to keep the port operation uninterrupted and safe. Moreover, data outflow must be controlled and restricted to minimize any unauthorized information leakages that would jeopardize the safety and security of the port operation. Information such as shipment schedule and cargo types should be properly guarded as these are high value targets for informational operations. It is also the intent of the system to educate the employees to achieve a knowledgeable workforce that is aware of the implication of security.

Some outputs are not intended and are by-products of the system. The by-products include employee dissatisfaction, restriction in personnel movement, and reduction in productivity. By implementing physical and informational access control, reduction in the rate of personnel movement and productivity would result. This may have a negative impact of the job satisfaction of the employee.

d. Functional Analysis

The functional hierarchy helps identify the most important functions of the system and decompose these functions into sub-functions. The primary concern of internal threats in the port is when an insider assists outsider(s) to execute terrorist acts within the port, or activities that support terrorist acts at other locations. The solution will have to address three fundamental functions of deter, access and response as depicted in Figure 119.

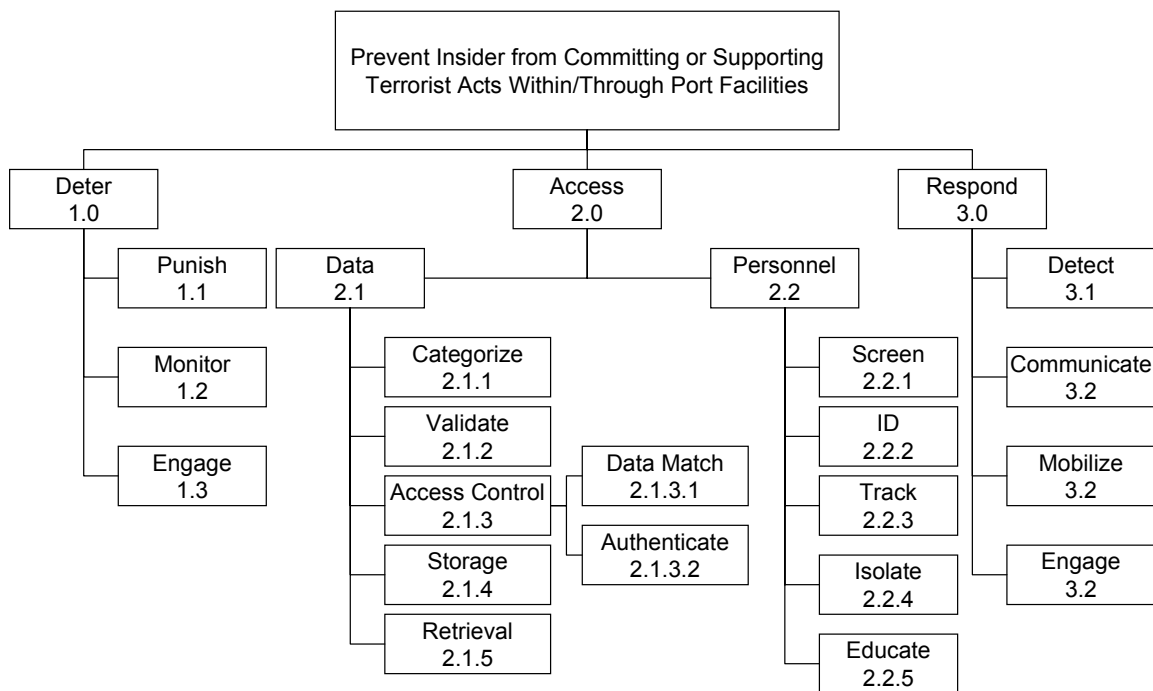


Figure 119. IPTG Functional Hierarchy

The first function that has to be addressed is how to deter personnel from collaborating with terrorists. To further explore this idea, the term deter can be thought

as a function that provide disincentive for anyone who acts to the detriment of the port. Subsequently, the deter function can be decomposed into three sub functions: setting barriers, monitoring, and engaging. The idea of having a physical fence or barrier might seem trivial, but it does provide a visual deterrence to a potential intruder. At a minimum, it would retard the breach of security and set a boundary for area layer defense. More effectively, it would require the intruders to formulate a work-around plan to breach security, and possibly be directed where the port defense is strongest. Once a barrier is established, monitoring would be required to ensure that the integrity of the barrier is maintained. Monitoring would also act as a first set of sensor that triggers an alarm system. (An alarm system with loud noise distributed over a wide area can be an effective deterrence method that prevents intruders from executing their activities once they realize that their intentions are no longer secret.) If a breach of security is detected, the sub-function of engage is to provide visual, audio, or other alarms as a last resort to deter the intruders from carrying out their intention.

Once the barrier is established to deter intruders, the next function that the system must address is how to provide access to both the information and the physical area of the port authority to those who have the legitimate need for such. The question of access can be divided into two sub areas: data and personnel. For data access, the primary concern is with the security sensitive data (and possibly, economic sensitive data). To further explore data access, a process needs to be established to categorize the sensitivity of the data. In addition, the data need to be validated to assess its integrity, and to facilitate establishing an access control method whereby the data is matched to those personnel who has a valid needs and their needs have been authenticated. However, as a way to minimize disruption to the port operation, a streamlined procedure is needed to prevent possible bottlenecks in either personnel authentication or data validation process. To ensure the safe keeping of the data, a robust storage with redundancy is also required, and a method of retrieving the data for the personnel also needs to be addressed. The main questions are: Can the data be accessed electronically and remotely? How many sites can the data be accessed through? The function of providing access for port authority personnel can be decomposed to: screening, identifying, tracking, and isolating.

In-coming workers should be screened for early determination of security risk. In addition, each worker should be provided with a unique ID that is tamper proof. Geographically, the port is generally a vast area. Providing access to personnel would also necessitate the need to track each worker to validate or authenticate their placement during their normal operating routine, and to ensure each worker is accounted for in an emergency situation. Lastly, once the access control procedure is established, a training method to educate the workers must be addressed to ensure everyone knows their security roles and responsibilities, and to keep security focus prominent to all involved.

Any security measure, regardless of their intended purpose, will experience lapses. Through extensive planning by intruders or unintended lapses by the system due to an unforeseen event, there are instances when the system will have to adjust to these events to maintain their effectiveness. The critical function at this point in time is response. More precisely, how does the system respond to a low probability but potentially catastrophic event, or to high probability but inconsequential events due to human or system errors? To further assist in understanding the function of response, it can further be divided into detecting, communicating, mobilizing, and engaging. When the security is breached, the system should have a method of detecting when and where it occurred. The information then needs to be shared and communicated with all involved. If and when a threat is validated and determined to have cataclysmic consequences, internal and external resources will have to be mobilized to neutralize the threat. At a minimum, even when a threat is determined to be attributed to human error, the internal resources should be mobilized to either validate that it is inconsequential and/or to reset the detection sensors. In the event that the threat is authentic, the security has been breached, and resources have been mobilized, an established set of rules of engagement are required to assist both internal and external security assets to determine each asset's roles and responsibilities in responding to each threat. For example, the rules of engagement would determine whether the internal security asset can detain or neutralize a threat prior to the external security asset's arrival.

2. Objectives Hierarchy

The objectives hierarchy is similar to the functional hierarchy, except this includes evaluation measures or metrics used to measure how well different alternatives meet the objectives. In addition, it also includes system attributes that are not functions but are nevertheless important decision criteria. The hierarchy begins with an effective need divided into the major functions, sub-functions, and metrics. Recalling the IPTG results from the needs analysis, our effective need is to prevent insiders from committing or supporting terrorist acts inside the port facilities. The three major functions and one objective of our system are to minimize impact to current operations, provide deterrence, control access to information and physical locations, and respond if necessary.

The primary function of the terminal port is to facilitate the movement of cargo to support both national and global commerce. The transportation of containerized cargo is a low margin, labor intensive industry with very minimal overhead. With the current global threat of terrorism, the port terminal operators and authorities are well aware of the security risks they might encounter. However, as explicitly stated by our stakeholders, security measures must not impede the commerce. Given this high order objective, the IPTG perceived it is important to our stakeholders that our solutions will have a minimal impact on the overall port operation. One perceived method to ensure that the IPTG doesn't lose sight of this critical requirement of the system is to directly place it in the objective hierarchy.

Unlike the other objectives which are linked to the system functions, this particular objective is essence represented attributes of the systems. As an example, non-performing characteristics can be factors such as ease of use, maintainability, or reliability. These factors were more designed to determine how well the system adapt to the environment that it is designed for. Attributes were also referred to as the 'ilities' of the system. These non-functional characteristics of the system provided important information to the stakeholders in deciding which alternatives to select. To help clarify the overall objective of minimize operation impact and to facilitate defining the meaningful metrics for this objective, the IPTG further decomposed into sub-objectives: operational delays due to implemented security procedures, the cost of the security

procedures, the operational complexity of security procedures, and the downtime of the security system. The impact of these sub-categories was to bring about a feasible solution, while minimizing the impact to the port's bottom line. Some metrics that we identified were the mean travel time of personnel, the average time to process a container, training time necessary, and system reliability. The alternatives that sufficiently address these metrics will be best for the IPTG system.

The next objective is to deter. Under the deter section, the three sub-objectives are to minimize the perceived accessibility, and to maximize the perceived detectability and the perceived intervention capability. The impacts of these sub-categories is to be maximized in order for all personnel to perceive that access cannot be achieved without detection and intervention will come before their plan can succeed. The metrics that were identified are number of attempted breeches and measurement of perceived security (which may be accomplished through surveys or expert opinion).

Another objective is to control access. Controlling access has been further subdivided into data and personnel categories. The objectives of data access control are to prevent information leakage, unauthorized access to information, contraband and/or dangerous substances from entering under fraudulent documentation, and to minimize the scope of information access to personnel. The personnel access control has objectives of preventing unauthorized physical access, minimizing the scope of access to personnel, and preventing inadvertent release of critical information. These categories of access control are to be maximized on a need to know or access basis in order to minimize the impact any single individual can have on operations. Metrics have been identified such as the number of unauthorized accesses, number of personnel who have access to data or locations, misidentification rate, and the number of successful attacks.

The final objective is to respond. The sub-objectives are to minimize damage after an incident and to minimize the time from incident to full operational recovery. Some metrics are time to recovery, amount of unrecoverable information, quantity of information leaked, time to detect, time to communicate, and time required to intervene. The objectives hierarchies are listed in Figures 120 through 123. The associated metrics are listed in Table 74.

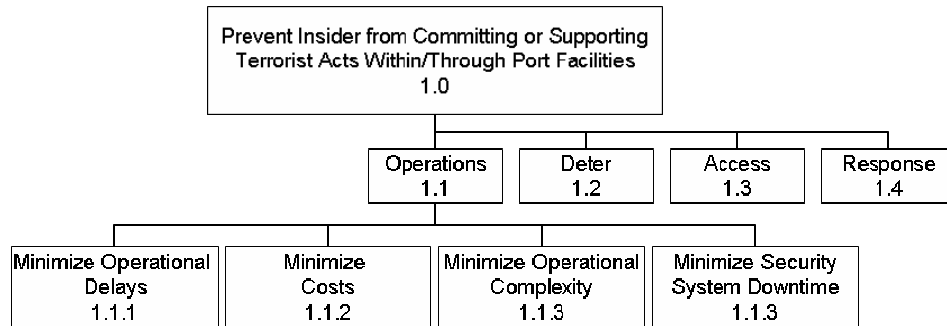


Figure 120. IPTG Objectives Hierarchy for Operations

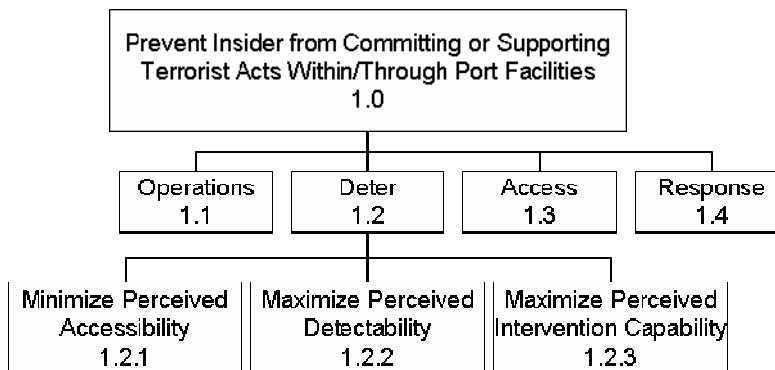


Figure 121. IPTG Objectives Hierarchy for Deter

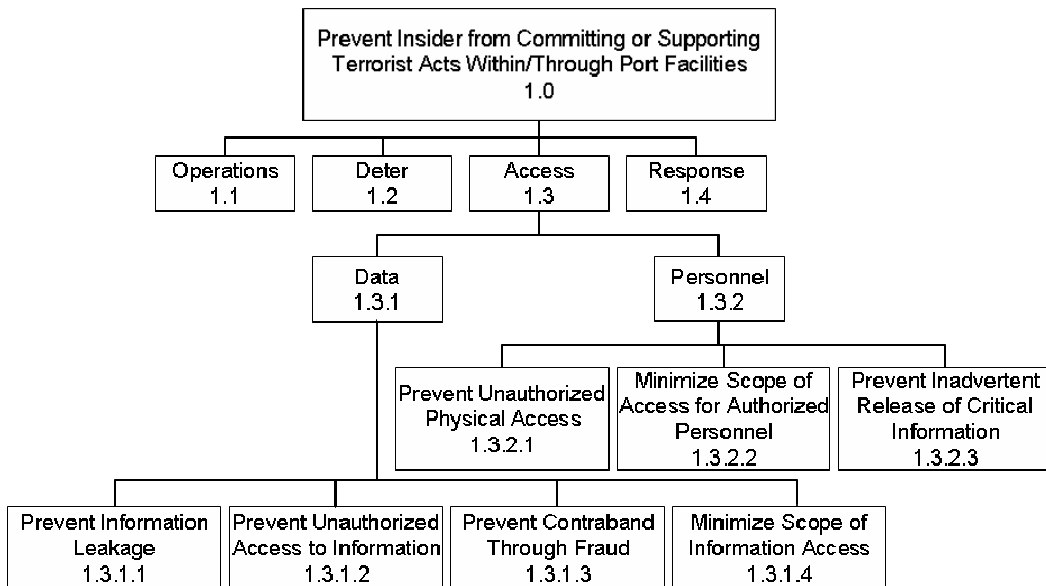


Figure 122. IPTG Objectives Hierarchy for Access

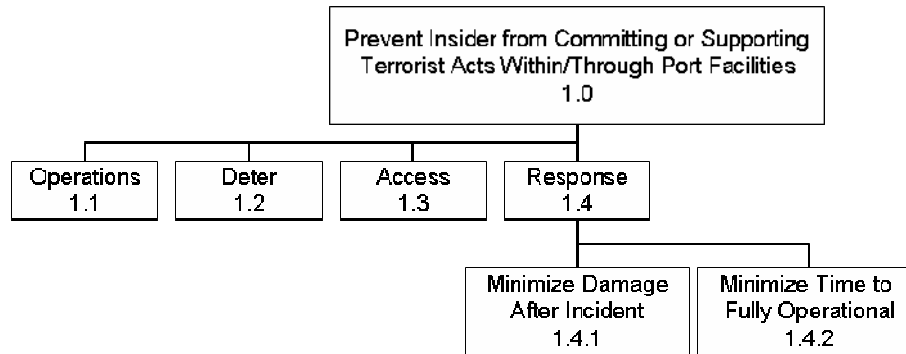


Figure 123. IPTG Objectives Hierarchy for Response

Metrics	Objective Item
Mean Sojourn Times (Personnel)	Operations - 1.1
Processing Time per Container	
Cost of System	
Time to Train	
Mean Time Between Failures of System	
Mean Time to Repair System	
Number of Employees Leaving Company per Month/Year	
Number of Complaints per Month/Year	
Number of Attempted Breaches	Deter - 1.2
Measurement of Perceived Security (Surveys, Opinions)	
Number of Unauthorized Access	Access - 1.3
Number of Personnel who have Access to Data/Locations	
Misidentification Rate	
Number of Successful Attacks	
Time to Achieve Normal Day to Day Operations	Response - 1.4
Amount of Unrecoverable Data	
Quantity of Information Leaked	
Time to Detect an Irregular Event	
Time from Detection to Communicating to Proper Personnel	
Time to Intervention	

Table 74. IPTG Evaluation Metrics

B. DESIGN AND ANALYSIS

1. Alternatives Generation

To support the formulation of the solution, the IPTG spent considerable effort gathering information initially from within the group, relying on the knowledge of the port operations based on interviews with the Port of Oakland Security Team and the PSA. Subsequently, extensive efforts were also devoted to online research, review of existing documents, and team discussion to familiarize ourselves with the security issues the port

authorities have to address. The IPTG segregated the specific issues that relate with the internal security of the ports concentrating on the port employees or infrastructure. In addition to the regular discussions held among the IPTG members to derive to the optimal solution, engagement with the stakeholders (Port of Oakland and PSA) attempted to validate selected methods to ensure that the approach to the problem was correct. In this regard, positive feedback was received from the two primary stakeholders. From the engagement of the stakeholders, the IPTG concluded there were differences in priorities and approaches to the same problem between the stakeholders. Their differences will be discussed further as their current security plans are analyzed in the search for solutions.

The approach to finding the solution begins with constructing a functional hierarchy of the problem. From the functional hierarchy, it was determined that to be successful, the solution must address how to perform each one of these vital functions effectively. The overall solution requires that each function must be independently addressed. The tool used to assist in this process is Zwicky's Morphological Chart.

The morphological chart is shown in Table 75 with each function listed in the column headings. Beneath these headings are the design alternatives or the means to carry out the listed function. For example, the function deter was listed in the first column as a heading. In the context of internal security, the objective of this function is to prevent or discourage outsiders from gaining unauthorized access to the port critical infrastructure and/or its critical data by discouraging port employees from acting on behalf of criminal and terrorist elements.

DESIGN ALTERNATIVES	DETER	ACCESS		RESPOND				
		DATA	PERSONNEL	COMM	MOBILIZE		NEUTRALIZE	
					Personnel	Eqt.	Non-lethal	Lethal
	VISUAL	PHYSICAL SECURITY	BIOMETRIC ID	PHONE	JET SKI	BOAT	PHYSICAL RESTRAIN	FIREARMS
	AUDIO	TRAINING	BACKGROUND CHECK	RADIO	FOOT	BARGE	CONTAINMENT	GAS
	PSYCHOLOGICAL	ENCRYPTION	LIMITED ACCESS POINT	DATA NETWORK	VEHICLE	TRUCK	TASER	
	PHYSICAL	BACKUP	MONITORING	VISUAL COMM	BOAT	TRAIN	RUBBER BULLETS	
	SIGNS	2 FACTOR AUTHORIZATION	GUARDS	HAND SIGNALS	HELO	PLANE	NETS	
	FENCE	NETWORK SECURITY	FENCE	PA SYSTEMS	BICYCLES	HELO	HIGH POWER MICROWAVE	
	WORD OF MOUTH		TURNSTILE	ALARM SYSTEM	MOTO	FORK LIFT	TEAR GAS	
	MONITORING		RANDOM CHECKS		GOLF CART		GUARD DOGS	

Table 75. IPTG Morphological Chart

Deter

There are three primary methods of deterring personnel from attempting malicious activity: punishment, denying access, and monitoring. Deterrence by punishment is a strategy which utilizes the possibility of apprehension of the attacker and punishment to the full extent of the law. The attacker is deterred if he chooses not to attempt his malicious activity because the perceived punishment is excessive. Deterrence by denying access aims to deny attackers opportunities to act. The attacker is deterred upon recognition that he does not have a good opportunity for attack and concludes that his probability of success is low. Deterrence by monitoring utilizes sensors or people to monitor the assets being protected. The attacker is deterred by the knowledge that he is being adequately monitored in an attempt to attack the asset.

The minimum requirement for deterrence requires all three of the previously mentioned forms. The following were selected as they serve their function with cost effectiveness. Deterrence by punishment could be carried out with warning signs. Signs posted at regular intervals along the perimeter fence, warning attackers that the port and terminal is being monitored at all times and unauthorized access would result in prosecution to the fullest extent of the law. The presence of armed guards reinforces these signs that would warn the attackers. Deterrence by denying access can be accomplished

by using perimeter fencing. This provides the minimum form of physical barrier to prevent and delay unauthorized access to the port area. Fencing also serves to channel the flow of personnel and vehicle to an access control point for effective screening. The minimum level of fencing is the wire-mesh crowned with barbed wire. Deterrence by monitoring may be accomplished via security patrols. A highly visible security patrol is an effective form of deterrence and is both versatile and capable of engagement. A well trained security patrol would be on alert for people acting suspiciously as well as search for objects that are out of place in relation to their surroundings.

Physical security can be further enhanced by legislation, dual layered perimeter fences, automatic vehicles barriers, security training, and an intruder detection system. Increasing the penalty for unauthorized access to the port area could be examined if the current penalty is unable to attain the desired level of deterrence. Allowing armed guards in the port should be examined as another forceful form of deterrence. Having a dual layer of perimeter fencing would not only effectively delay the attacker, but also provide a clear area between the inner and outer fence for any sensor system to be optimized for detection and monitoring. Lighting could be provided throughout the fencing to help prevent night intrusion. To prevent drivers from ramming their vehicle through the access point, an automatic vehicle barrier could be implemented. Typically, the response time for the security guard to activate the barrier would be small and hence concrete blocks to slow down vehicle speed could be utilize to allow these automatic vehicle barrier to be effective deployed. The best form of monitoring is the vigilant awareness of the people working in the port. Through training, there would be increased vigilance by the workers, enabling them to report any suspicious activities or people to the security agents. Through regular training, the workers could feel safer working within the port and understand that they are an integral part to the security plan. To supplement security patrol, an intruder detection system could be employed. These systems can sense any cut in the fence, tunneling under the fence, or attempt to scale the fence. Installation of these systems reduces the workload of the security patrol and is another form of deterrence.

Data Access Control

To effectively protect against information threats, security measures placed in order to protect the accessibility and integrity of data are of prime importance. Such measures span across a broad spectrum of domain knowledge, including areas such as physical security, network security, cryptography, access control, and business continuity planning. While each of these areas achieve some specific sets of goals, it is important that careful considerations be given when implementing these measures to achieve a robust layered approach to effectively handle the various informational threats.

In order to achieve basic data access control, it is necessary to implement a set of measures that will form the essential baseline to protect the critical data from unauthorized access. One of the basic requirements in dealing with informational threats is to ensure that the premises where data are stored or accessed are secure. This can be achieved via implementation of basic physical security measures, which typically include measures to deter, delay, detect and response to physical threats. To effectively implement such measure, a centralized approach in the data resource management is preferred, and one such approach is the consolidation of data resources to the data center, in which tight physical security measures can be implemented and enforced. A typical data center is well protected by layered defenses such as security personnel, barriers and locks. This would deter and delay any potential adversary. Intrusion monitoring and detection are achieved via motion detectors and CCTV. A data center could have a set of emergency response processes and escalation channels should any compromise in security is detected. With such centralized approach to physical security, the chances of data compromise are greatly reduced compared to a distributed approach. While the data centers are being physically secured, it should be noted that adversaries can still access the data via the network. To address such threats, network security measures need to be put in place. Such measures include the use of firewalls to inspect and block unwanted network traffic, the implementation of demilitarized zones (DMZ) to buffer against attacks on critical information assets. At a minimum, storage encryption at the personal computers should be implemented to protect the confidentiality of the data used by the employees. Such measure ensures that any adversary would not be able to access

sensitive information easily even if they manage to gain access to the files. With all these measures in place, it should not be forgotten that robust access control mechanism could be in place to prevent unauthorized access of the data. The basic mechanism should include individual authentication and authorization via the use of user IDs and passwords. Auditing of user access should also be enforced to ensure traceability and accountability. A basic set of requirement to ensure business continuity is to have at least a formal set of backup and recovery procedures for the critical data. The backup data should be stored offsite. These measures ensure that there is at least a working set of data should the integrity of primary source of data be compromised.

The baseline data access control will form the basic safeguarding mechanism. To achieve a more robust data access control, it is necessary that more measures be put in place to re-enforce the baseline mechanism. Apart from the basic set of physical security measures, a guard post and monitoring post could be set up at the entry point to the data centers. Procedures to control the inflow and outflow of data to the data center by checking all storage media carried by the personnel entering or leaving the data center must be strictly enforced to prevent any unauthorized access or leakages of information. Vendors performing installation and configuration of servers within the data center should also be escorted at all time. The data center should be situated in a hardened facility to ensure that it is protected against physical sabotage by any potential adversary. Besides implementing the DMZ and firewalls, network-based and host-based intrusion detection and prevention systems could be implemented to detect and react to any attacks. Such systems would be monitored continuously by information security professionals in order to ensure fast and appropriate response. From examination of the large premises of a maritime port, the bits and bytes during wire transmission may also be vulnerable to sniffing and attack. The use of cryptography such as secure socket layer (SSL) and public key infrastructure (PKI) would be able to address such threats. Storage encryptions should also be implemented at the servers to protect the confidentiality of critical data in the data center. The use of two-factor authentication such as biometric or smart card for data access should be enforced to achieve a more robust access control mechanism. Such mechanisms could be linked with physical access control so that only authorized

personnel are able to access the critical data resources within the data center. Finally, business continuity planning ensures that critical data are backed up periodically and an alternative site will be available to restore the backup data should the primary site fails for some reason. A set of policy and procedures are to be established and periodically exercised to test the procedures to be executed to ensure the data can be restored in the event of attack resulting in loss or corruption of data.

Respond

The Port of Oakland is taken as the baseline for our considerations in port security, and thus its response capabilities form the minimum level required. Threat may be detected in the administrative area (offices), operational area (storage, loading/unloading, berths) and perimeter of each terminal. The threat may be in the form of an intruder, authorized visitor (including trucker) or terminal employee. The jurisdiction of the terminal is limited to visual monitoring and verbal warning to the threats. There is a heavy reliance on the local authorities for any actions required to neutralize the threat. The local authorities would most likely be activated from their nearest station and travel in cars and trucks. At the perimeter, the threat would be denied entry and monitored by terminal's security personnel. Local police would be called via telephone to apprehend the threat. In the administrative area, the office personnel may call his superior for appropriate actions. Security personnel may be required to escort the threat to the perimeter and hand over to local police. For uncooperative cases, the local police may be called to make arrests. There could be a need to evacuate the building in a situation in which the threat carries explosives or firearms. In the operational area, the watchman will inform (via handheld radios) the security personnel while monitoring the threat. The watchman could attempt to deny the threat from assessing the critical facilities. In the meantime, the local police are called to make the arrest. Again, for threat carrying explosives or firearms, there will be a need to evacuate the terminal personnel in the immediate vicinity.

The maximum response alternative explores the possibility of placing the emphasis on response capabilities, while meeting the minimum requirements in access control and deterrence. By response capabilities, we mean the abilities of the proposed

system to neutralize the threat before it can cause any damages to the port facilities or other landmarks through the port. Since the internal threat is primarily human-based, the response will be focused on how to neutralize the human threat most efficiently and effectively.

Upon detection and identification of threat, the response function would be triggered to neutralize the threat appropriately with minimum lag time. Handheld radios would facilitate communications among the security personnel during the response action. Alarm and public address systems would work in tandem to alert the terminal personnel to appropriately assist in the response either by keeping away or actively pursuing or cutting off the threat. In the near future, it is possible to broadcast the live picture and location of the threat's movement on TV screens at strategic locations or solely to the security personnel, so that it is easier to isolate the threat.

Physically, the terminal may be rigged to raise walls to segregate the terminal into sections to minimize the abilities of the threat to escape or reach the critical facilities. The walls would also minimize collateral damage to adjacent facilities. For example, such walls should be implemented in the container area to prevent the threat from hiding. External agencies would be called and the best response can be achieved if these agencies are stationed in the port vicinity.

Alternative One (Status Quo)

Due to extensive knowledge of its operations and its current security capabilities, the Port of Oakland is used as a baseline alternative. The advantages of using the Port of Oakland as the measuring yardstick are because they are familiar with the issues that have to be addressed; they know the challenges that have to be overcome, and the effectiveness of some of the solutions that are currently being implemented. Since the solutions are formulated for implementation five years out, the solutions are expected to be only slightly better than the current technology offerings.

For deterrence of unauthorized access into the port terminals, the Port of Oakland uses a multi-layered method. As one approaches the port terminal from the road, there are multiple visual and physical signs of deterrence: posted warning signs threatening

prosecution for unauthorized access, warning signs indicating that the fence is electrified, fences along the terminal perimeter, serpentine barbed wire on top of the fences, and CCTV along the perimeter. As a psychological deterrence, the access in and out of the terminal is zigzagged in an effort to confuse casual intruders presenting a tactical advantage. The zigzagged road pattern allows the guards the opportunity to monitor those approaching the terminal.

For data access control, the electronics data network servers and supporting equipment are located in three rooms on the ground floor of the terminal administrative building. The rooms are outfitted with electronic card readers, and access to the rooms is tightly controlled. The network itself is access restricted, with user login and password required for entrance. Personnel access is authorized based on their job functions. The network is highly compartmentalized and aligned to each personnel job tasks. For example, planners have access to data about incoming ship containers with their manifests, then electronic applications are designed specifically to allow them to formulate the most optimal stacking arrangement.

As for personnel access to the terminal, there is only one personnel entry point to the terminal. At the entry point, there are two electronically activated turnstiles; the turnstiles are activated by the Transportation Workers Identification Credentials (TWIC) card. There are CCTV monitors mounted over the turnstiles with full redundancy, two monitors are pointed at the entrance of the turnstiles, two at the exit. Located past the turnstiles is a guard post. Personnel have to bypass the guard post to gain entrance to the terminal. The guard provides the final verification of incoming personnel. The guard can also de-activate the turnstiles to allow visitors or employees without a TWIC card to come through the turnstiles. However, as a security procedure, the guard must verify and validate all visitors. All visitors require escorts.

For responding to security breaches, personnel can mobilize within the terminal by 15-person van, pickup trucks, and golf carts. For equipment, pickup trucks and forklifts are available within the terminal to be used to move concrete barriers, and or temporary fences. If all the deterrence methods fail to prevent intruders from gaining access to the port, and if security is compromised, as a final measure, the CBP agents

assigned to the port terminal carry firearms and are federally authorized to use them as necessary.

Alternative 2 (The Port of Singapore)

Deterrence is the primary measures that the port of Singapore undertook in the port security plan. A strong deterrence factor cuts the desire to attempt malicious activity. Visually displaying security personnel and instructions or equipment are ways to enhance the deterrence factor. It will be effective to have security personnel patrolling everywhere with watchful eyes to safeguard the security of the port. In addition to the human fatigue problem, tremendous labors cost makes it unwise to impose such deployment. Optimized numbers of security personnel are deployed around the port to patrol the grounds.

Together, large signboards displaying the “Trespassers will be prosecuted” and “Area under surveillance” warned the implications of any wrongful actions with the sublime message of “everyone is watching and we are ready to catch you.” These signboards are prominently placed and spread across the surrounding fence line of the port premises. Fence lines are built around the surrounding compound to cordon off the premises from public access is one physical measure undertaken. Limited access points with security screening helps to sanitize the port premises. Since the port is a large area, it is not possible to have security patrol within every inch of the port areas.

The use of technology is an important component in aiding the security capability. CCTV with smart video analyzing software is the latest device to aid in securing the compound. Currently, the Port of Singapore is well-equipped with such an intelligent surveillance CCTV system that monitors each sector of the compound and looks out into sea and land channels to thwart any undesirable actions. Again, the display of such sophisticated camera all around the compound and fence will inform and warn any further deliberation of opportunistic threats. Some of the undesirable actions that can be detected are trespassers, irregular flow of traffic (people, vehicular, container) directions, irregular behaviors (loitering, break-in etc).

Other complimentary technology along the fence could be the installation of tripwires in secluded areas. Typically, audio alerts are placed together to summon all the

necessary attention for action to be taken. Publicizing the capability of certain security implementation is also another form of psychological combat to weave off any undesirable attempts and increasing difficulty for any sabotage plans. Therefore, the Port of Singapore does display robust security capability which shows strength in the safeguarding of the port.

As for access control of data, shipping information is critical information safeguarded by the port of Singapore. Only authorized personnel have access to the docking and scheduled information. The information is compartmentalized to declassify it to the necessary stakeholders such as transportation companies, handlers and shipping lines. Only necessary information is distributed to the grounds at short notice to prevent any planned sabotage. Information regarding the placement of scheduled duties for crane operators, ground handlers and even checkpoints officers are also highly guarded. All data access requires access cards to verify the authenticity of the information retriever. Network security and encryption are also imposed on the data information. Since the Port of Singapore handles one-fifth of the world's total transshipment throughput, a complete port operation backup and data disaster recovery has been implemented to ensure business continuity.

Personnel access control is performed via identification by the issuance of photo access cards. Different levels of access control are implemented and controlled by the access cards. Guards are stationed at key access points. Other places, such as administrative offices, require two factors of authentication such as the swiping of access cards and keying in of passwords. All the access information are logged and screened for any irregularity such as late night or early morning access to administrative zones or storage areas. Vital equipment, such as cranes, need special authorization to access. All personnel must display their access pass prominently in all zones as security guards or employees are vigilant for any unauthorized access. Biometrics identification at all access points are set to authenticate personnel. The implementation would lengthen the time taken to screen the personnel which is significant in the port where the large working population exists, and efficiency is a key factor. Currently the biometric screening is only activated when a certain threat level is issued by the HSAS. To safeguard port security

against insider sabotage, background checks are conducted on all contractors and staff permitting issuance of only relevant authorizations. All contractors (including handlers, drivers, and caterers) have to submit personnel information for clearance prior to entry. No entry will be given if prior notice is not served. Security guards at the guard post will authenticate and verify the information with the contractor's employer. Personnel such as ship's crew members are classified as immigrants and proceed under the discretion of the ICA.

In the case of a security breach, the response forces augment the port security personnel with the Singapore Police Force (SPF), Singapore Civil Defence (SCDF), PCG and RSN. In the premises of the port, the PSA's security force would be the first responders. To initiate security response, multiple points of activation that range from personnel or the triggering of an alert by surveillance system are available. There is a recall management system that electronically mobilizes security force to the scene via their localized intercommunication system and even their mobile phone if they are outside the port area. Being the first responders, the security force of PSA would be mobilized to the scene. Assessment would be done to decide if any further activation of relevant authority and expertise is required. Once the threat is validated, methods and equipment used to neutralize the threat are evaluated. Guards armed with batons are taught engagement techniques. If the threats are armed, SPF would be involved in the engagement with firearms. If there is a chemical, biological, radiological or explosives threat, the SCDF will be activated as they are trained and specially equipped to handle such threat.

Alternative 3 (Maximizing Response)

This alternative explores the possibility of placing the emphasis on response capability, while meeting the minimum requirements in access control and deterrence. Response capability is the ability of the proposed system to neutralize the threat before it can cause any damage to the port facilities or other landmarks within the port. Since the internal threat is primarily human-based, the response will be focused on how to neutralize the human threat most efficiently and effectively. Threat may be detected in the administrative area (offices), operational area (storage, loading/unloading, berths) and

perimeter of each terminal. The threat may be in the form of an intruder, authorized visitor (including trucker) or terminal employee. To achieve maximum response capability, it is necessary to monitor and neutralize on the threat swiftly and comprehensively during the response phase. The concept of operation requires the terminal to actively restrain the human threat while external agencies are activated. The terminal should be equipped to neutralize the threat to a limited extent, if necessary prior to the arrival of external agencies. This can be achieved by communication, mobilization, and neutralization.

Upon detection and identification of a threat, a response function would be triggered to neutralize the threat within a minimum amount of time. Handheld radios would facilitate communications among the security personnel during the response action. Alarm and public address systems would work in tandem to alert the terminal personnel to appropriately assist in the response either by deterring or actively pursuing and neutralizing the threat. Through the network of CCTVs installed throughout the terminal, the movement and action of the human threat can be monitored. In the near future, it is possible to broadcast a live picture showing the threat's movement on monitors at strategic locations or broadcast to the security personnel via Personal Digital Assistants (PDAs), enabling the identification and isolation of the threat. Ideally, there would be more than one security command & control centers on the terminal (and even off-site) to provide redundancy. In addition, one of the centers could be designated to track the current human threat, while the remaining centers can continue to search for other threats. This will ensure that distraction tactics would not be successful.

Internal security personnel would be stationed at strategic locations throughout the terminal, rather than at a centralized location. They would be equipped with bicycles to facilitate their movements and to carry their equipment, reducing their response time. In addition, training a portion of the terminal personnel should be considered to assist the established security forces. A sufficient number of trained pseudo-security personnel (similar to the watchmen in Port of Oakland) well dispersed throughout the terminal during normal operations would ensure a rapid response on human threats. External agencies would be called and the best response would be achieved if these agencies are

stationed in the port vicinity. Otherwise, the external agencies should patrol the port vicinity with sufficient frequency to provide first response prior to the main force. In addition, there would be some robust yet swift means of verifying the identities of the external agencies prior to entry. This could be as simple as an e-mail from the external agencies providing information on the key personnel that are dispatched. The e-mail would be accessible by the security personnel at the gate instantaneously. As a backup, direct numbers of external agencies should be listed at the guardhouse. This is to prevent the intentional tripping of the security system in the terminal to facilitate the entry of falsified personnel from external agencies.

The security personnel within the terminal would be armed with non-lethal as well as lethal means to neutralize the human threat. The non-lethal means may include rubber bullets, tear gas and nets. Pseudo-security personnel would assist to neutralize the human threat, and are not expected to physically restrain the threat. However, they may be equipped with tazers for self-protection. Physically, the terminal may be segregated into zones to facilitate ease of neutralization. The means of segregation are fences, walls, and gates. Upon alert, the gates could be closed automatically to limit the human threat to certain zones. The pseudo-security personnel may assist to prevent the human threat from scaling the fences. Guard dogs could prove effective at chasing human threats due to their speed, ability to sniff out their locations and psychological effect on the human threat. Hence, it is recommended to have guard dogs in the response plan.

C. MODELING AND ANALYSIS

1. Modeling Plan

In modeling the internal personnel, we have introduced various models to model and simulate the design; in deterrence capability, data control and response.

For deterrence capability we will use a mathematical model based on Mr. Robert Anthony's analysis of the deterrence against the 9/11 terrorists was used [67]. For control access capability, the IPTG used a combination of models to analyze both the access control capability of information and personnel. For personnel, a probability based model was generated to analyze the ability of the access control alternatives to thwart internal

personnel smuggling in explosives, and the impact of the access control plan on the process flow of the port terminal operation.

For data control, leveraging prior academics analytical works whereby a combination of a stochastic model to simulate the randomness of network intrusion occurrence [68] in conjunction with the Markov decision process to analyze the security of the IT infrastructure system was used [69]. Lastly, an agent-based model (i.e. MANA) was used to analyze the response capability with the focus on assessing the communication channel effectiveness of the coordination between port security officers and the local and federal agencies.

Each model was designed to simulate a particular function of the IPTG's system design. The link among all the models assessed two performance characteristics: the probability of catching internal personnel in the act of sabotage and the qualitative assessment of the probability of deterrence. The parameters and the outputs of the models are listed below in Table 76.

	Modeling Tool	Input Parameters	MOEs Obtained
Deter	Excel	1. Probability of apprehension 2. Severity of consequences for offenders	1. Probability of deterrence
Physical Access	Extend	1. Probability of detection for various detection measures 2. Delay time associated with each detection measures	1. Probability of detection 2. Mean delay time 3. Cost of system
Data Access	Excel	1. Probability of detection at various points of data access	1. Probability of detection 2. Cost of system
Response	MANA	1. Quality of communications 2. Existence of internal fence	1. Probability of interdiction 2. Cost of system

Table 76. IPTG Model Input Parameters and Associated MOEs

2. Modeling Explanation

a. *Deterrence Model*

The basis of the deterrence model was the logical assessment that the terrorists who are engaged in a high-risk venture must constantly exercise caution. Even suicide terrorists, who generally hope to conduct significant attacks, would most likely not carelessly or recklessly squander their lives on an attack that had little chance of success. From Mr. Anthony's 9-11 report, to accomplish the 9-11 attacks, the terrorists had to successfully perform nine sequential tasks from organize, plan, recruit, train, getting passport, learn to fly, board the planes, and to crash the planes while avoiding military aircraft interception. At every step the terrorists had to assess their success rate and decide whether or not to proceed. On the same token, every step also presents an opportunity for interception or detection of the terrorist plot to prevent it from continuing. The deterrence model examined this terrorist execution process qualitatively and quantitatively, explored the missed opportunities for deterrence, and assessed whether the behavior of the 9-11 terrorists suggested, even if momentarily, indicators of deterrence in their final decision to proceed.

The model was formulated and calibrated with data from the Drug Enforcement Administration (DEA) narcotics interdiction operation in South America. The general deterrence relationship was described by the mathematical model shown below,

$$P_t = 1 - (1 - P_t)W(P_t^*)$$

where,

P_t - the probability of thwarting crime

P_t - actual probability of being apprehended

$(1 - P_t)$ - the probability of not being apprehended

P_t^* - criminal's perceived probability of being apprehended

$W(P_t^*)$ - the willingness to do the crime

For simplicity, it was assumed that the perceived of apprehension, P_t^* , was the same as the actual probability of apprehension, P_t . This assumption could be checked or modified as needed for specific situations. To calibrate the willingness factor,

empirical data collected from drug interdiction was used to extrapolate into factors for our own deterrence model. From the interdiction data, it was found that the willingness function is an inverse power function that relates three general characteristics of the psychology of deterrence:

For the low probabilities of apprehension, there was a minimum threshold below which perpetrators ignore the risks, but beyond which many were deterred.

The initial threshold for deterrence was determined by the perpetrators' perceptions of the consequences of getting caught, and those consequences were set by interdictors' rules of engagement.

There was also a residual fraction of perpetrators who were never deterred by the given consequence, and it equals the deterrence threshold probability.

Subsequently, the fitted willingness function had the relationship below:

$$W(P_i) = \left(\frac{P_i}{P_o} \right)^{-1.03 \pm 0.2}$$

where,

$P_o = \text{Threshold}$

The exponential factor of -1.03 +/- 0.2 reflected the calibration factor of the consequence on psychological deterrence. The value of -0.83 (-1.03 + 0.2) indicated a low consequence of getting caught, i.e. material loss or an equivalent misdemeanor punishments, whereas the value of -1.23 (-1.03 - 0.2) indicates a high consequence of getting caught, i.e. loss of life or life imprisonment.

To apply the mathematical model to assess the deterrence capabilities of various alternatives, the output of the model was dependent on three variables: interdiction probability, consequences and punishment of getting caught, and the threshold of deterrence. The interdiction probability was highly dependent on the personnel access control model. The security placement and screening would play a pivotal role if internal personnel could be caught doing something detrimental to the port terminals. The probability of interdiction would be subjectively assessed based on

qualitative evaluation of the various personnel access control measures. The consequences factor would be assessed based on site specific data by applicable laws governed the ports, which was calibrated to reflect the MARSEC level. For example, if someone is caught by the CBP during MARSEC level III would be more harshly punished as opposed to someone caught by the port authority security officer during MARSEC level I. Lastly, the threshold of deterrence was a qualitative assessment of the baseline security infrastructure currently implemented by the port security.

b. Physical Access Control Model

The Physical Access Control Model was used to determine the probability of successful attempt by an internal threat whose objective was to bring explosives to a target of interest within the terminal without being detected. The additional delay induced in the flow of movements for other terminal workers due to various alternatives was also recorded.

The model was separated into two parts: gate access and unauthorized movement within the terminal. In the gate access portion, the model simulated the arrival of 70 terminal workers including the internal threat who was carrying explosives. All the workers had to enter the terminal through the turnstiles. This was modeled for the morning rush when everyone was arriving for work. The flowchart in Figure 124 depicts the process of the gate access.

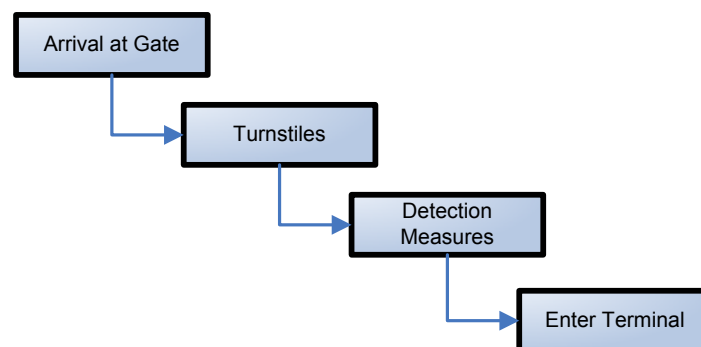


Figure 124. Gate Access Flowchart

All workers including the internal threat was required to enter the terminal through the turnstiles where they were subjected to various measures such as walk-through metal detectors and bag scanners.

In the unauthorized movement part, the model simulated the movement of the internal threat from the admin building towards the target of interest. Along the way, the threat would encounter varying number of personnel who would question his movement. This process is depicted in Figure 125.

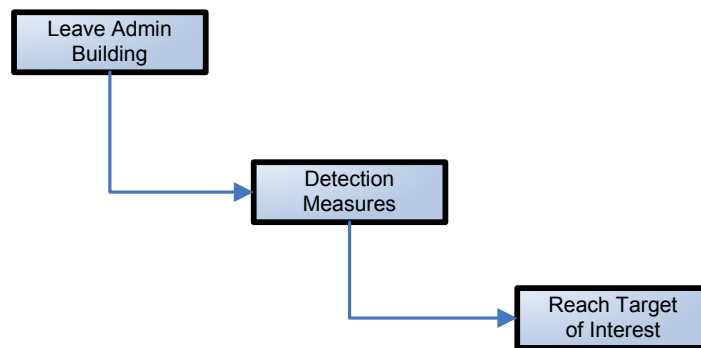


Figure 125. Unauthorized Movement Flowchart

The internal threat would leave its place of work in the Admin Building and walked towards the target of interest with the explosives. The threat attempted to avoid various detection measures such as watchmen and security personnel.

The underlying assumptions were as follows:

- The internal threat would bring in the required explosives only on the day he intended to execute his plan.
- The exact nature of the explosives was not modeled, but it was assumed to be detectable with certain probability.
- Since the probability of detection for various measures could not be convincingly determined from open sources, the team attempted to give a reasonable figures to the various parameters associated with each detection measures.

The distribution of arrival time for the 70 workers was assumed to have the form as shown in Figure 126. The internal threat was assumed to consistently arrive around 0745 hrs at the gate, with the majority of workers to avoid being conspicuous.

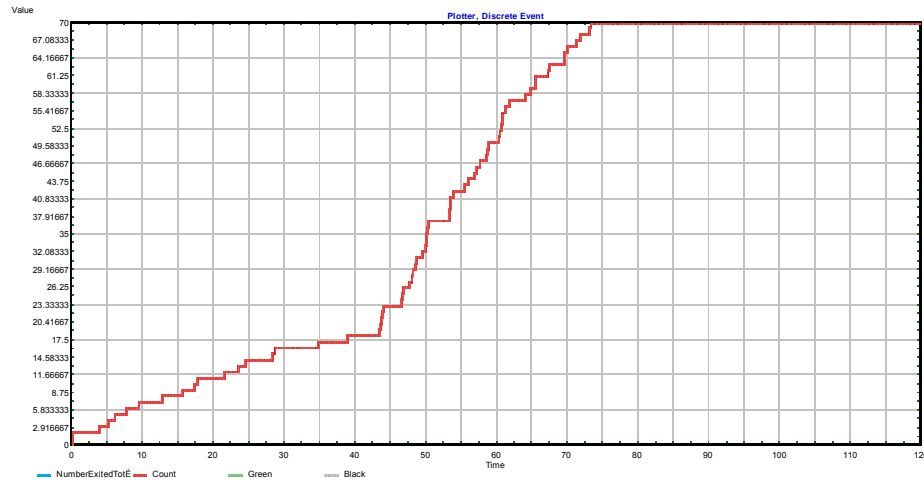


Figure 126. Distribution of Arrival at Gate

Assuming the first worker arrived at 0700 hours, and the last worker at 0810 hours. The majority of the workers were expected to arrive between 0740 hours and 0810 hours.

The key parameters for the model were the time taken for various activities and the probabilities of detection using the various means. These are summarized in Table 77. Note that these were arbitrary, but assumed reasonable values.

Activities	Mean Values	Standard Deviations
Clearing Turnstiles	Delay time – 15 secs	2 secs
Random Checks by Guards	Probability of being chosen – 0.10	0.05
Random Checks by Trained Guards	Probability of normal workers being chosen – 0.10 Probability that internal threat was chosen – 0.3	Normal workers – 0.05 Internal threat – 0.15
Walk Through Metal Detector and Bag Scanner	Probability of detection – 0.50 Delay time – 30 secs	Detection – 0.10 Delay time – 5 secs
Bag Search and Hand-held scanner	Probability of detection – 0.80 Delay time – 60 secs	Detection – 0.10 Delay time – 10 secs
Watchmen	Probability of detection – 0.20	0.05
Security Personnel at Internal Fences	Probability of detection – 0.50	0.10

Table 77. IPTG Model Activity Parameters

The model was simulated for 1,000 runs with each alternative. The outputs from the modeling were as follows:

- Probability of detecting the explosives carried by the internal threat.
- Additional delay induced due to the various detection measures implemented.

The MOE provided was the probability that the internal threat managed to bring explosives from outside the terminal and activated at his target of interest without being detected. This is calculated from the model output as follows:

$$\begin{array}{lcl} \text{Probability of success} & & \text{Probability of detection} \\ \text{(by internal threat)} & = 1 - & \text{(by the terminal)} \end{array}$$

The Physical Access Control Model was a queuing model using ExtendTM v6.0.2. The parameters were hard-coded into the model prior to each run, and the outputs were read off and recorded. Each alternative was simulated with 1,000 runs.

c. Data Access Control Model

The approach for modeling data access control was divided into two parts. The first part of the model was developed using a network representation of the system structure together with Markov models of intruder progress and strategies. This model provided an explicit mechanism to estimate the probability of successful breaches of information infrastructure security as well as to evaluate potential improvements. The second part of the model was based on a probabilistic decision tree that modeled the various components that were part of the infrastructure security. These two models combined to provide a more comprehensive view of the system robustness.

In the first part of the data access model, a Markov decision process was constructed to model the intruder's strategy at the system level, without carrying along all the details of each state of the process.

At the system level, a network of barriers and movements for an insider trying to obtain sensitive information were represented using a set of nodes and arc, as shown in Figure 127.

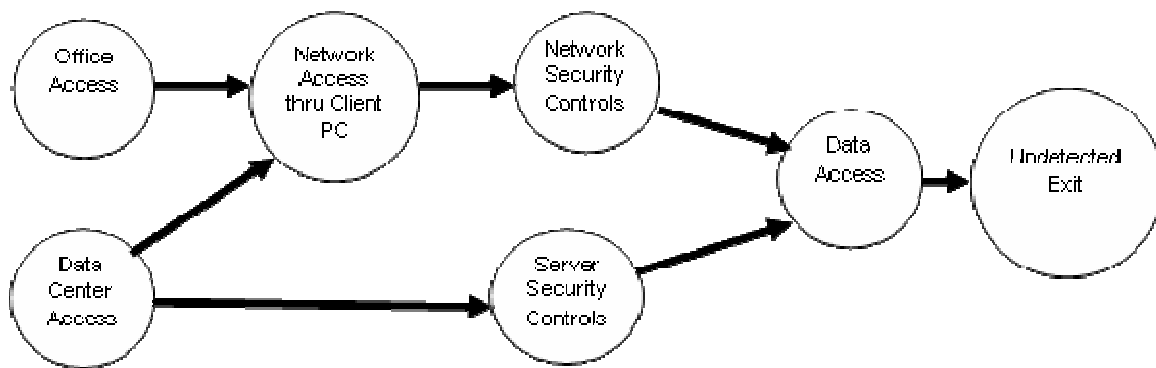


Figure 127. System Level Network

In Figure 127, the nodes represent barriers that an intruder must penetrate, and arcs represent movements between barriers that an intruder can make within the system. If an attempted penetration at a particular entry node is successful, they can traverse edges from the successfully breached node to other nodes in the network that are connected to the one breached, which entails a risk of detection.

As an insider, the intruder must first gain access to the data through his own office, or he may attempt to directly go to the data center facility. After physical access has been gained, he may attempt to gain access to the network through a client PC terminal, or directly go to the server if he is within the data center. Network access entails negotiating the network security controls such as firewall and network intrusion detection systems, while direct server access requires the intruder to compromise the server security controls such as lock in the rack. Once access has been gained, the intruder would need to gain access to the data by breaking the access control of the data. Once the data has been obtained, he would attempt to exit the facility without being detected.

A set of input data on the probability of success and probability of detection for the various nodes and arcs give rise to the solution for the intruder strategy as summarized in Figure 128. To the left of each node is the probability of a successful attack', given that the intruder is arriving at that barrier. To the right of each node is the probability of success, given that the intruder had successfully negotiated that barrier.

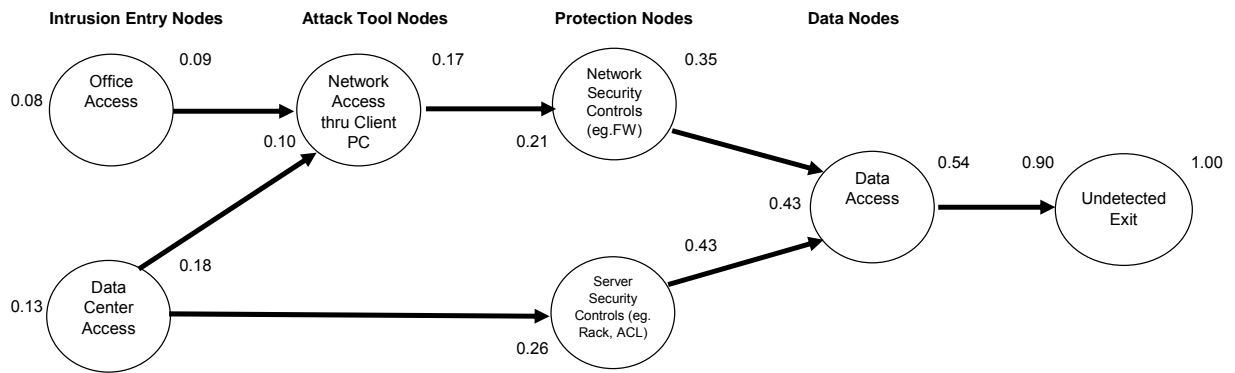


Figure 128. Summary of Intruder Strategy and Probability of Success

Figure 128 established the base-case for the system. With the base-case, a series analysis can be performed by varying the various inputs to the network to examine the impact of potential changes to improve security. For example, attempts could be made to reduce the probability of a successful attack on highly sensitive servers by housing them in separately secured rooms with an additional CCTV system. The impact of such additional security features on the overall probability of success could be investigated.

In the modeling of the various alternatives, parameters of the various nodes and arcs have been varied to investigate the various differing levels of security applied to the port environment.

The objective of the second part of the data access model was to facilitate the understanding of the key components in the design alternatives for Personnel Access Control. Particularly, in the analysis of data information access by personnel, the key components were physical security, training, encryption, backup system plan, authorization mechanism and network security.

The model sought to use probabilistic theory to statistically model a relationship between the design of the key components and their aggregated effect towards an effective implementation of the design. A simple way to look at the model was to use Game Theory (from the perspective of the threat): a mathematical and economical analysis to decide the decision path. From the implementer point of view, it was a layered defense in information assurance. Basically, the analysis started with the

nature of traffic in the design i.e. an insider threat with a probability of success associate with each key component in placed by the design. Each key component was represented by a node that characterizes the probability of successful entry by the traffic (insider personnel). For example in the diagram below, an insider has a 0.2 probability of accessing a data center access compared to a $(1-0.2) = 0.8$ probability of logging thru an office network and hack through the system to retrieve the desire data. Figure 129 depicts a probabilistic model of data access associating with the design of components.

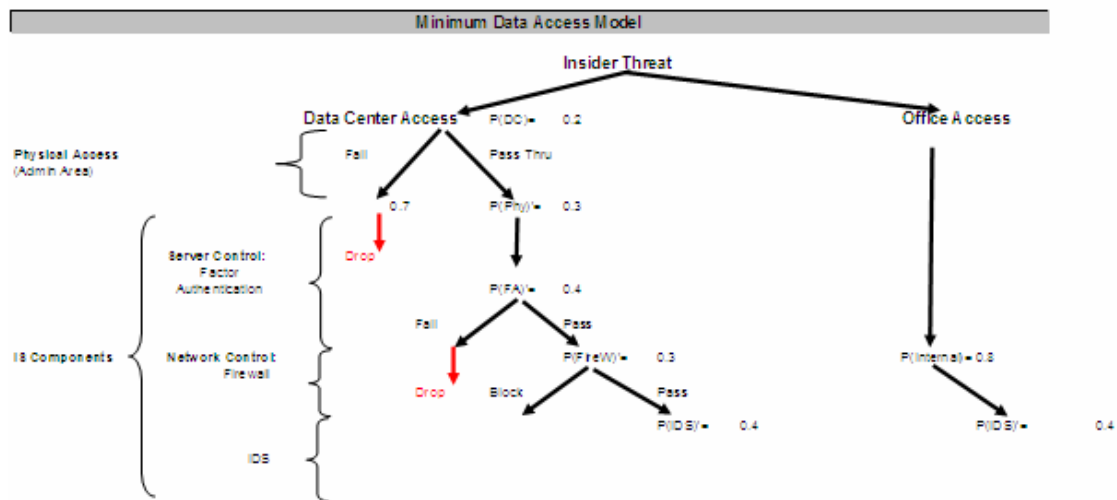


Figure 129. Probabilistic Data Access Model

The decision on the design alternatives were based on the state (intrusion with signal or no signal) derived from results using Bayes rule as illustrated in Figure 130. However, it should be noted that at this stage the model did not try to accurately pinpoint the probability of success an intruder based on the probability of success (or capture) by each key component (defense layer). On the other perspective, the results revealed the effectiveness of introduction of design alternative in the data access control logic.

BOX 1. BAYES RULE.

$$\eta_1 = \frac{P(\text{intrusion}|\text{signal})}{P(\text{signal}|\text{intrusion})P(\text{intrusion}) + P(\text{signal}|\text{no-intrusion})P(\text{no-intrusion})}$$

and

$$\eta_2 = \frac{P(\text{intrusion}|\text{no-signal})}{P(\text{no-signal}|\text{intrusion})P(\text{intrusion}) + P(\text{no-signal}|\text{no-intrusion})P(\text{no-intrusion})}$$

Figure 130. Bayes Rule

Lastly, the model used random distribution to simulate the randomization attempts by an insider intruder via the threat path to determine the average probability of success in the design model.

Markov Model - Minimum Design Scenario for the Port of Oakland

In modeling the insider threat, a set of input data on probability of success and probability of detection of the various nodes and arcs was needed to determine the overall probability of success. Table 78 shows the node data used for the analysis and Table 79 shows the probabilities of detection used for the arcs in Figure 129. The values are hypothetical, with the aim of illustrating the relative importance and relation to each other values within the network. In practice, these input values would likely be a mixture of estimates based on specific elements of the targeted system.

Node	Prob of Success	Prob of Detection
Office Access	0.90	0.10
Data Center Access	0.70	0.30
Network Access thru PC	0.60	0.40
Network Security Controls	0.60	0.40
Server Security Controls	0.60	0.40
Data Access	0.80	0.20
Undetected Exit	0.90	0.10

Table 78. Data for Network Nodes (Minimum Scenario)

Arc	Prob of Detection
Office Access - NW Access thru PC	0.10
Data Center Access - NW Access thru PC	0.30
Data Center Access - Server Security	0.30
NW Access thru PC - NW Security	0.20
NW Security - Data Access	0.20
Server Security - Data Access	0.00
Data Access - Undetected Exit	0.40

Table 79. Probabilities of Detection for Possible Move (Minimum Scenario)

With this set of data, it is shown that the probability of success for intrusion through normal access is 0.08 compared to a probability of success of 0.13 for intrusion through gaining access to data center. Hence, an intruder with insider information would choose to intrude through the data center, and this scenario would give an upper bound to the probability of success with the input data considered.

To explore the effect of varying the various controls of the nodes, a “what-if” analysis could be conducted, i.e. what if more server security controls are put in place. The next part of the report attempts to describe the scenario with maximum data access control to illustrate the point. Figure 131 depicts the probably of success for the minimum scenario.

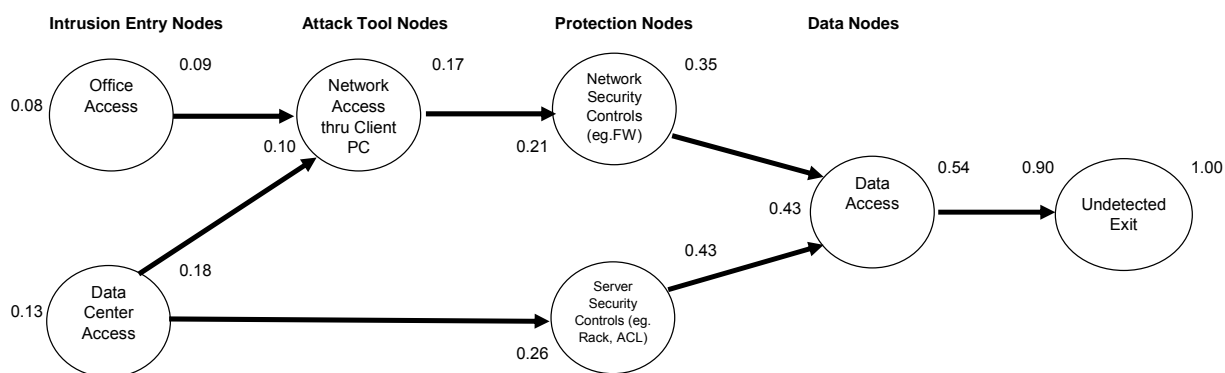


Figure 131. Probability of Success for Minimum Scenario

Markov Model - Maximum Design Scenario for the Port of Singapore

In the maximum design scenario, it is assumed that mechanisms have been placed to reduce the probability of success of all the nodes as well as to increase the probability of transversing the nodes. Table 80 shows the node data used for the analysis and Table 81 shows the probabilities of detection used for the arcs.

Node	Prob of Success	Prob of Detection
Office Access	0.90	0.10
Data Center Access	0.60	0.40
Network Access thru PC	0.50	0.50
Network Security Controls	0.50	0.50
Server Security Controls	0.50	0.50
Data Access	0.70	0.30
Undetected Exit	0.80	0.20

Table 80. Data for Network Nodes (Maximum Scenario)

Arc	Prob of Detection
Office Access - NW Access thru PC	0.15
Data Center Access - NW Access thru PC	0.35
Data Center Access - Server Security	0.35
NW Access thru PC - NW Security	0.25
NW Security - Data Access	0.25
Server Security - Data Access	0.00
Data Mining - Undetected Exit	0.45

Table 81. Probabilities of Detection for Possible Moves (Maximum Scenario)

The resultant probabilities of success are shown in Figure 132. It can be seen that by tightening all the controls of the nodes and arcs, the probabilities of success can be significantly reduced to 0.03 for office access and 0.06 for data center access.

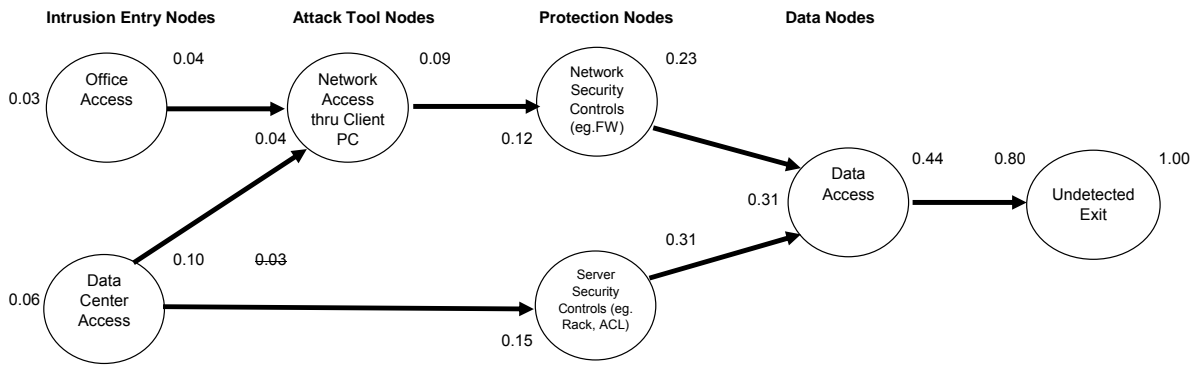


Figure 132. Probability of Success for Maximum Scenario

Markov Model – Other Design Scenarios

The Markov decision process allows the modeling of any other design scenario by performing a “what-if” analysis on the various nodes and arcs. The effect of varying the control mechanism within a node or arc on the overall probability of success of intruding into the system can then be studied. For example, it may be desirable to tighten the server physical security mechanism by requiring all works done on the server to be escorted by a system administrator. This would serve to reduce the probability of success at the server security node, thereby decreasing the overall rate of success of intruding through data center access. A numeric example is not given here, as there are numerous possibilities that one can explore given the user specific set of operating environment.

Probabilistic Model – Minimum Design Scenario for the Port of Oakland

The parameters considered are as follows:

- Physical security of servers
- Network security
- Access authentication & authorization (One FA authentication)
- Backup data

The input parameters for the minimum design scenario are specified in Table 82.

Access Personnel	P(office)	0.8
	P(Data Center)	0.2
Physical Access	P(Phy)	0.7
IS Components	P(FA)	0.4
	P(FireW)	0.7
	P(IDS)	0.6

Table 82. Input Parameter for Minimum Scenario

With the above parameters, the results are generated using the probabilistic data access model. In the minimum design scenario, the parameter value was extracted from internet research (www.secunia.com) on overall effectiveness of each typical components of security infrastructure based on market survey. Key assumption made here was the holistic effectiveness of an basic authentication system with One Factor Authentication of 0.4 value. The results of the simulation are as shown in Table 83.

Data Center Access		
P(intrusion/no signal)		0.00432
P(intrusion/signal)		0.00648
Office Access		
P(intrusion/no signal)		0.32
P(intrusion/signal)		0.48
Results		
Avg P(Success)	1FA(0.4)	0.216877

Table 83. Results for Minimum Scenario Simulation

The results have shown that:

- The layers of implementation of physical security, factor authentication and network security control greatly reduced the probability of intrusion. (Comparing data centre access and office access).
- The insider threat through office access is a good chance (32 percent) of intruding and going undetected. On the hand, 48 percent will be detected.

Probabilistic Model - Maximum Design Scenario for the Port of Singapore

The parameters considered are as follows:

- Physical security of servers (Biometric)
- Network security
- Cryptography (SSL & PKI)
- Access authentication & authorization (2 FA authentication)
- Backup data

The input parameters for the maximum design scenario are specified in Table 84.

Access Personnel	P(office)	0.9
	P(Data Center)	0.2
Physical Access	P(Phy)	0.7
IS Components	P(FA)	0.6
	P(FireW)	0.7
	P(IDS)	0.8

Table 84. Input Parameters for Maximum Design Scenario

In this scenario, the design template increases the physical security access, network security and intrusion detection security components. This results in having a higher probability of detection in both the Access control and Information Security components sections. The results of the simulation are shown in Table 85.

Data Center Access		
P(intrusion/no signal)		0.00072
P(intrusion/signal)		0.00288
Office Access		
P(intrusion/no signal)		0.18
P(intrusion/signal)		0.72
Results		
Avg P(Success)	1FA(0.6)	0.111649

Table 85. Results of Maximum Scenario Simulation

The maximum design scenario tightens the overall implementation effectively. The results have shown that the detection capability have almost doubled,

which means that this aspect of the concept of layer defense has a high effectiveness. In simulating a multiple randomization of intruder, the average success for an insider threat is approximately 11 percent.

d. Response Model

The Response Model was an agent-based, Map Aware Non-uniform Automata (MANA) version 3.2.1. The parameters were hard-coded into the model prior to each run, and the outputs were stored in excel. Each alternative was simulated with 100 runs. The response model was used to determine the probability of that an internal threat who successfully penetrated the access control measures could reach the desired target. The Response Model will reflect the ability of the personnel stationed within the Port Terminal to prevent the perpetrator from reaching the target once the access control plan produces a signal. Due to the force-on-force nature of the response plan, MANA was the software chosen to best model the response capabilities.

The response model is dependent on the infrastructure and trigger points of the Access Control phase. Therefore there are multiple scenarios that must be created in MANA in order to fully analyze the alternatives. There will be eight independent scenarios ran in MANA: 1) Baseline, 2) Improved Communications, 3) Mid-terminal fence with perpetrator starting at main entrance gate, 4) Mid-terminal fence with perpetrator starting at main entrance gate with improved Communications, 5) Mid-terminal fence with perpetrator starting at main entrance gates and mid-terminal gates triggered shut, 6) Mid-terminal fence with perpetrator starting at main entrance gates and mid-terminal gates triggered shut with improved communications, 7) Mid-Terminal fence with perpetrator starting at mid-terminal gate, and 8) Mid-Terminal fence with perpetrator starting at mid-terminal gate with improved communications.

The underlying assumptions were as follows:

- The internal threat would proceed directly from point of successful access control breach to the critical target.
- Due to the relatively short amount of time required to traverse the terminal, outside personnel would not arrive in time to prevent the perpetrator from reaching target. Therefore, they are not included in the model.

The terminal map was taken directly from the highest resolution image available on Google Earth. This map was then simplified using color schemes allowed by MANA for denoting terrain. Table 86 denotes how terrain was modeled:

Real Port Items	MANA Color	Represented in MANA as:
Pavement/ Concrete	Yellow	Roads
Containers, Equipment, Terminal boundaries, Building walls	Grey	Walls
Building interiors, and area underneath cranes	Light Green	Light Brush
Interior Fence	Dark Green	Dense Bush

Table 86. Response Terrain Model Description

The key parameters for the model are the attributes used to model communication. Also, there were other attributes that are significant enough to note. The attributes and how they were modeled are listed in Table 87.

Real Attributes	Modeled in MANA as:
Baseline Communication	All agents appear on matrix. Inorganic SA Range set to 50 m
Improved Communication	All agents appear on matrix. Inorganic SA Range set to 1000 m
Federal Agents- Weapon: Gun	Range to Shooter: 200 m Hit Rate: 0.3 Range to Shooter: 10 m Hit Rate: 0.8 Range to Shooter: 1 m Hit Rate: 1.0 Note: Interpolation enabled Note: Can't fire through walls or hills selected
Guards, Watchmen, Perpetrator- Weapon: Unarmed (fists)	Range to Shooter: 1 m Hit Rate: 1.0
Perpetrator's path to target	Waypoints used

Table 87. MANA Model Attributes

The model was simulated for 100 runs with each alternative. The outputs from the modeling were the probability of successfully interdicting the perpetrator before target reached.

The MOE provided was the probability that the internal threat managed to bring explosives from outside the terminal and activated at his target of interest without being successfully interdicted. This is calculated from the model through MANA's Excel output.

3. Modeling Results and Analysis

There were two threat scenarios that the IPTG analyzed: an employee smuggling in explosives to cause physical damage to the ports and an employee extracting vital port operation or security data to be used against the port.

Four complimentary models were generated to aid in validating solutions to each scenario. For the first scenario, where personnel attempt to smuggle and/or detonate an explosive in the port, an EXTEND model was created. This model was used to simulate a port employee in the process of entering the port terminal just before the commencement of regular working hours. Various alternatives were analyzed to determine the effectiveness of each in catching an employee in an attempt to smuggle explosives. Using the Port of Oakland as the status quo, turnstiles requiring ID badges for access and guards monitoring the process were simulated. The same model was used to simulate other alternatives improving the probability of capturing the employee in the act of smuggling. The two additional physical access control options analyzed were: the inclusion of metal detectors in conjunction with random search procedures similar to the process TSA use with air transportation and having guards specifically trained in identifying suspicious activities. Different alternatives with various mixes of the two options previously mentioned were analyzed. The composite layout with all the options implemented is illustrated in Figure 133. For nomenclature, we referred to the alternative with the inclusion of all the options listed as Max Access Control.

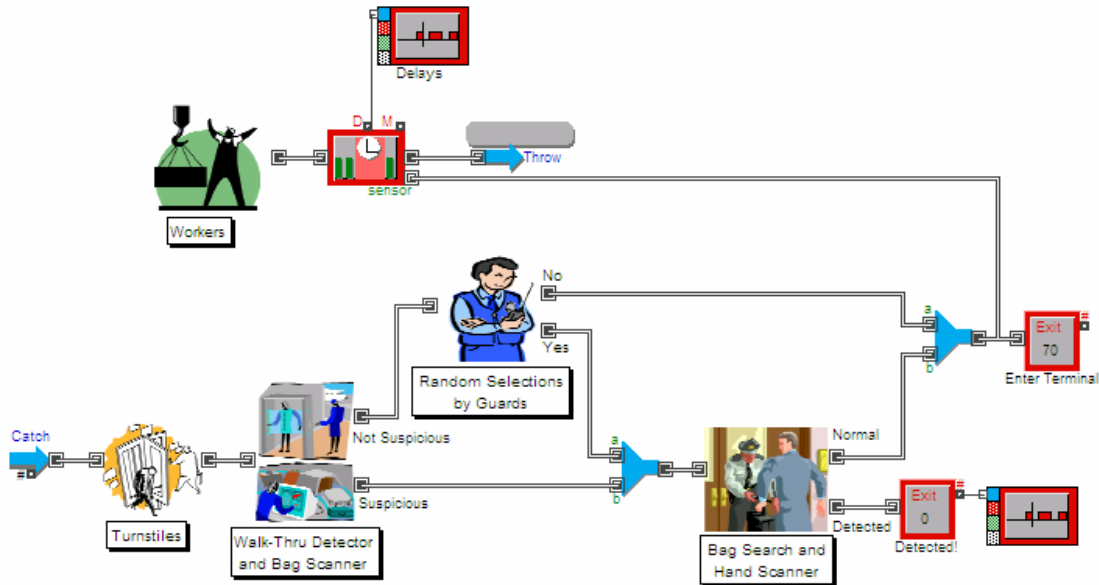


Figure 133. Physical Access Control EXTEND Model

Given the conditions described previously, the expected results of the EXTEND model were that the personnel would be detected at the terminal entrance point. However, to analyze the port terminal's layered defense, an agent based model was created using MANA to simulate the response plan in the event that the perpetrator managed to get the explosive through the entrance point, but not before the guard activates the port terminal's alarm. The perpetrator would attempt to continue the mission by running for the designated critical target such as a crane on offloading radioactive medical supplies from a ship docked at the pier. In this analysis, the alternatives that were analyzed were the effectiveness of the port security internal communication system among the guards, watchmen, and the CBP as they consolidated their efforts in stopping the personnel from reaching his objective. In addition, the effectiveness of installing a fence between the container storage area and the loading/off-loading cargo area, which will limit and restrict access within the terminal operational area, was analyzed. The fence had three access openings to allow for people and cargo to move from the operational to the storage area illustrated in Figure 134. At each opening of the fence, there was a guard positioned to check ID and verify access clearances. An optional alternative was to explore the effectiveness of having the fence gates opened or

closed during alarm the conditions. For modeling the closed condition, if detection occurred at the terminal entrance, then the gates to the mid-terminal fence would be activated to close. The intent was to stop or retard the rogue personnel from reaching his objective through the critical access points which lie beyond the fence.



Figure 134. MANA Model with Internal Fence

Figure 135 on the following page depicts the communication links utilized in the MANA Model.

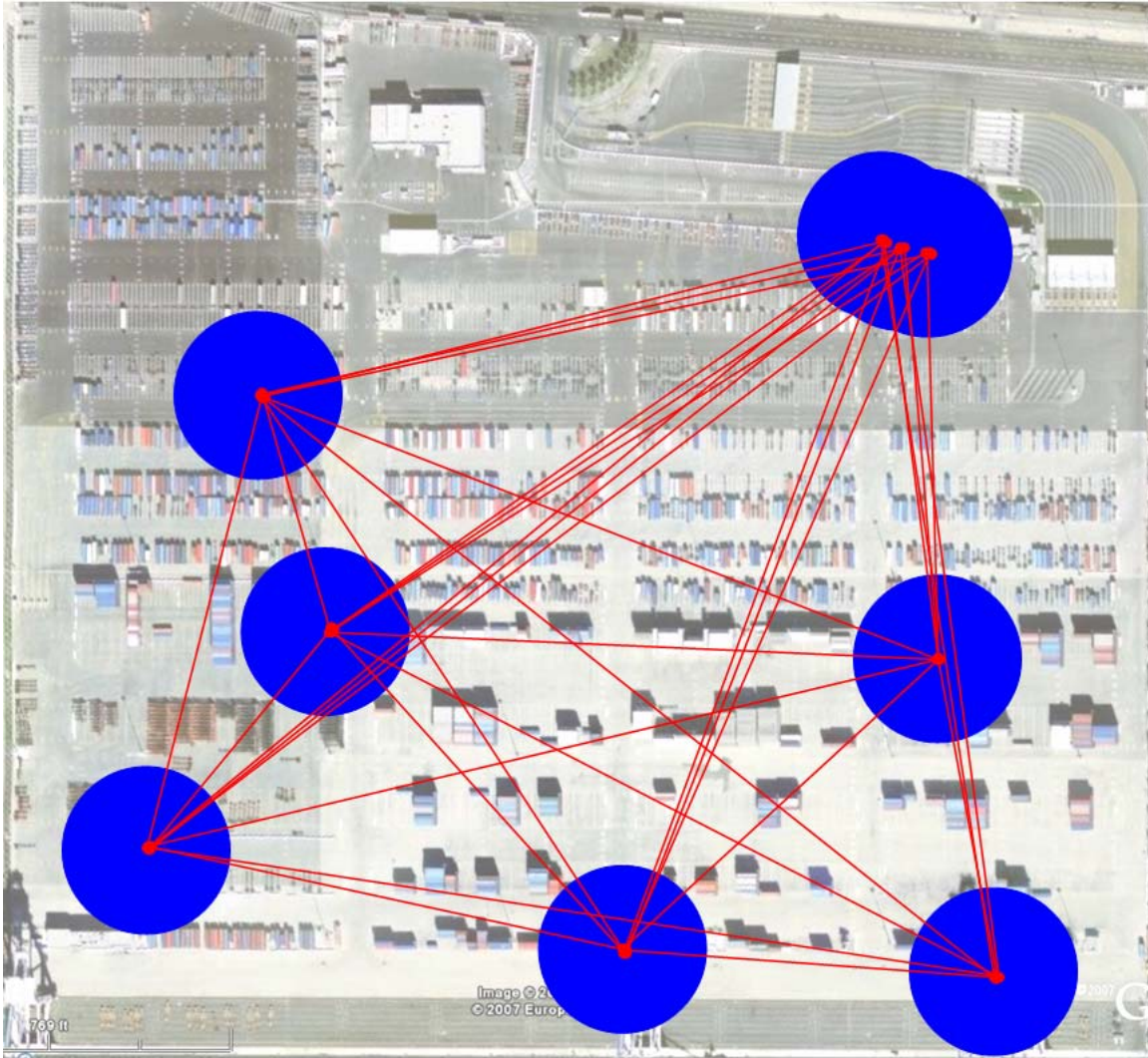


Figure 135. MANA Model Denoting Communication Links

For the data access control model, an EXCEL spreadsheet was used to model the process the rogue employee must use to gain access to critical unauthorized data. The focus for the EXCEL model was to assess the effectiveness of the physical security of the computer servers containing the data, and assess the effectiveness of deploying a two-factor authentication system for network security. The EXCEL model is shown in Figure 136.

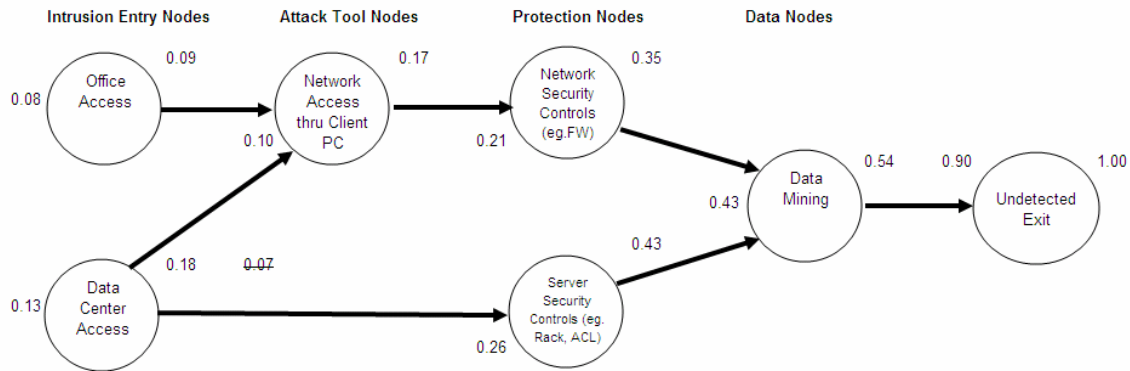


Figure 136. EXCEL model of Data Access Control System

The results of the EXTEND physical access model is tabulated in the Table 88.

$P_{\text{Detection}}$	Without Internal Fence	With Internal Fence
Status Quo	.343	.669
Untrained Guards	.392	.694
Trained Guards	.497	.747
Max Control	.681	.839

Table 88. EXTEND Model Results

The results that were obtained from the MANA model of the response tended to be as expected. The raw data is listed in Table 89.

Scenario	P(Successful Interdiction)	% Improvement over baseline
No Fence, Poor Comms	0.32	0
No Fence, Good Comms	0.52	63
Fence, Open Gate, Poor Comms	0.63	97
Fence, Open Gate, Good Comms	0.77	141
Fence, Closed Gate, Poor Comms	0.48	50
Fence, Closed Gate, Good Comms	0.87	172
Mid-Terminal Gate Starting Point, Poor Comms	0.39	22
Mid-Terminal Gate Starting Point, Good Comms	0.54	69

Table 89. MANA Raw Data Matrix

Every improvement feature and combination of such features yielded significant gains over the baseline scenario. The presence of the mid-terminal fence with an open gate policy provided the largest single factor improvement of 97 percent over the baseline status quo. The combination of improved communications, mid-terminal fence, and a triggered-shut gate policy yielded the highest probability of successful response with a 172 percent improvement over the baseline.

It is important to note, however, that the probabilities listed above are dependent on a detection signal being produced by some aspect of the access control plan. Accordingly, the probabilities are only for responding to the threat once the threat is identified. Additionally, because of this, the mid-terminal gate starting point data can not be compared to the rest of the response plan results and were modeled only to combine with physical access data for a more complete analysis.

There was one apparent anomaly in the MANA response model. The scenario consisting of a fence with the gate triggered shut paired with poor communications actually produced a probability of successful interdiction lower than if the gate were kept open. This does not seem to make logical sense as the closed gate should make it sufficiently difficult for the perpetrator to pass which enables the responders to successfully interdict. However, it was not possible to correctly model the fence in MANA. This was primarily due to the fact that the value of terrain hindrance had to be spread over a thickness much greater than the thickness of a fence to achieve the same level of impenetrability as a fence. This affected the results as the responders had to travel through the fence to get to the perpetrator from both sides and through some meaningful thickness. Also, if the perpetrator were to cut his way through the fence, the responders would be able to use the same hole. In MANA, it was not possible to model this. There could be no easier path through the fence for the responders. Essentially the responders would then have to cut through the fence again. This same anomaly was not apparent with the good communications model as the responders were able to reach the perpetrator with great numbers and in shorter amounts of time, reducing this effect.

A final conclusion as to the effectiveness of any single improvement or combination of improvements cannot be based on the MANA results alone because of the

inherent dependence relationship with the physical access control plan. Accordingly, a more useful and thorough analysis is presented as part of the whole model analysis.

Due to the very high probability of successful interdiction that the baseline data access model produced, it is more useful to discuss the results obtained via the physical access and response models. Additionally, separating the data access allows for useful analysis and conclusions to be drawn from scenarios that do not require data access, which may be considered more probable. The baseline which models the current facilities and procedures at the Port of Oakland produced only a twelve percent chance of successfully detecting and interdicting a perpetrator attempting to enter and traverse the terminal. By implementing the same items listed in the complete model conclusions without the data access control model being considered, the successful detection and interdiction percentage increased from twelve percent to just over sixty-five percent (a 441 percent improvement). These results are somewhat masked when analyzed in the framework of the complete model and its associated scenario (Table 90).

P(Interdiction)			<i>Physical Access Control Measure</i>			
			Status Quo	Untrained Guards	Trained Guards	Max Control
No Internal Fence		Bad Comm	.1210	.1359	.1677	.2334
		Good Comm	.1816	.2068	.2609	.3557
With Internal Fence	Open	Bad Comm	.3068	.3311	.3828	.4735
		Good Comm	.4052	.4327	.4910	.5934
	Closed	Bad Comm	.2781	.2933	.3256	.3823
		Good Comm	.4243	.4579	.5291	.6542

Table 90. Combined Physical Access & Response Model Results

Consequently, the resulting interdiction probability of capturing the perpetrator in the act of committing terrorism fed the mathematical deterrence model which gave theoretical values for psychological deterrence. The resulting probabilities of deterrence are tabulated in Table 91.

P(Deterrence)			<i>Physical Access Control Measure</i>			
			Status Quo	Untrained Guards	Trained Guards	Max Control
No Internal Fence		Bad Comm	.9043	.9068	.9112	.9177
		Good Comm	.9128	.9154	.9198	.9253
With Internal Fence	Open	Bad Comm	.9227	.9241	.9266	.9301
		Good Comm	.9275	.9286	.9306	.9336
	Closed	Bad Comm	.9210	.9219	.9238	.9265
		Good Comm	.9283	.9295	.9318	.9351

Table 91. Psychological Deterrence of Implementing Access Control Measure

Our overall model, which combined the data access control model, physical access control model, and response model, produced results consistent with expectations. That is, each item that was expected to improve the security of the terminal actually did. Thus the conclusion was that the terminal should implement 1) two factor authentication for computer network access 2) improved communications for all guards, watchmen, and customs agents, 3) build a mid-terminal fence with gates that can be remotely shut, 4) provide additional training to guards/ watchmen, and 5) install metal detectors and bag scanners. By implementing the above items a thirteen percent increase was realized in successful interdiction rates over the baseline.

The probability of detection of the combined security features are listed in Table 92 below. Note the underlying assumption is that the perpetrators need to access critical network data prior to execution, and the results have shown that network data intrusion detection plays a critical role in interdicting the rogue employees.

P(interdiction)			One-Factor Authentication				Two-Factor Authentication			
			Status Quo	Untrained Guards	Trained Guards	Max Control	Status Quo	Untrained Guards	Trained Guards	Max Control
No Fence		BC	.815	.819	.825	.839	.903	.905	.908	.916
		GC	.828	.833	.845	.865	.910	.913	.919	.929
With Fence	Open	BC	.854	.860	.870	.889	.924	.926	.932	.942
		GC	.875	.881	.893	.915	.935	.938	.944	.955
	Close	BC	.848	.852	.858	.870	.921	.922	.926	.932
		GC	.879	.882	.901	.927	.937	.940	.948	.962

Table 92. Combined Total Probability Detection

The findings summarized that both the physical access control and response section generated a very low probability of capturing the intruder compared to the data access control section. Based on the results of the EXTEND model, it is recommended that to enhance the deterrence and physical control factors, metal detection gates and trained guards should be emphasized. As for the response section, the simulated MANA models suggested that an improved communication system will increase the guards' watchmen's collaborative efforts and resulted in greater effectiveness in responding to a security breach. The analysis resulting from the statistical model of data access control depicted the criticality of controlling information access to thwart (or reduce the probability of a successful attempt by an intruder) while maintaining adequate information assurance. The combination of the three models illustrated the concept and effectiveness of a defense-in-depth approach to port security for internal personnel access control –complimenting the three stages of the protection design; deterrence, physical and data access and lastly the response, will greatly enhance the effectiveness of the protection solution.

The modeling showed that the effects of implementing Two Factor Authentication (2FA) increased the security of data access by an additional 10 percent. A Two Factor Authentication system typically is composed of a smart card or token in combination with the traditional login-password system. Security analysts from the industry found that the traditional login-password system is weak and prone to dictionary attacks or even clever guess attacks. Therefore, with the implementation of 2FA systems, it is made more difficult with close possession of the smart card or token.

The other key point is the importance of good physical access control in information systems. It is the first and most important defense layer of the defense-in-depth concept. Modeling has also shown the deterrence probability with the implementation of this concept. Each layer introduced will reduced the probability of a successful penetration into the information system. Hence, it is recommended that the 2FA system should be implemented together with the concept of layers defense.

4. Cost Estimation

For cost analysis, an assumption was made that the security system would be installed and have an operating life cycle for 10 years, after which the depreciated value of the system will be fully depleted. All costs are depicted in CY 2007 U.S. Dollars.

For the data access control implementation of two factor authentication, a keyboard with ID badge reader would be required at the cost of \$100 per keyboard. Using Hanjin terminal of Oakland as a basis of our estimate with 20 administrative personnel, the resulting total purchasing cost is \$2000. In addition, modification to the port existing networks servers would also be required to allow for screening personnel, along with establishing network firewalls. For simplicity, IPTG assumed that the terminal operators would contract out the tasks of upkeep and support of the networks security system at the cost which was estimated to be a full time job for one Information Technology (IT) personnel. Consequently, the average hourly standard loaded wage rate for contracted IT personnel is \$37 per hour, the annual operating cost for maintaining a network security will be approximately \$74,000.

The component cost for implementing the physical security access control measures are broken down as follows:

Untrained Guard with Random Handheld Metal Detector Search

The cost of hand-held metal detector is \$1000 and the guard at the turnstile requires one hand held metal detector. There are no O&S costing related to this metal detector as it assume to have one year warranty and the highest cost associated with this option would be to buy one detector a year after the warranty period.

The total cost for this option would be $\$1000 \times 10 \text{ year} = \10K .

Trained Guard

There are seven existing guards in the terminal and their hourly wage is approximately \$50. For a security training package of one week, it would cost $\$50 \times 8 \text{ hr/ day} \times 5 \text{ days} \times 7 \text{ guards} = \14 K in man-hour. Hiring one trainer for one week would cost \$6K.

The total cost for this option would be $(\$14\text{K} + \$6\text{K}) \times 10 \text{ year} = \200K

Maximum Access

The metal detector gate and the bag scanner would cost \$150K with an O&S cost of \$15K per year. It is assumed that after 5 year, the metal detector gate and the bag scanner would be replaced.

The total cost for this option would be $\$150\text{K} + \$150\text{K} + (\$15\text{K} \times 10 \text{ year}) = \450K .

Fence with gate and guard

The cost of procuring and installing a fence was assumed to be \$100 per yard and 700 yard would be required, hence \$70K would be required for fencing. There will be three access control points with automatic gate that cost \$10K each with an O&S cost of \$3K a year. The total cost of the gates would be $(3 \times \$10\text{K}) + (\$3\text{K} \times 10 \text{ year}) = \60K .

It is assumed that three additional guards would be required to man the three gates. The cost of guard is \$100K per year. Over ten year, they would cost $\$300 \times 10 \text{ year} = \3000K .

The total cost of this option would be $\$70\text{K} + \$60\text{K} + \$3000\text{K} = \3130K .

Installing the fence along with the guards to implement the physical access control would also benefit the response plan. However, to fully deploy our response plan would also require upgrading the existing walkie-talkie with its range and capability limitations to a hot microphone system similar to those used by the personnel security professionals and SWAT teams, which priced to \$3000 per unit. The total number of units required was estimated to be 24 which also include spares and replacement costs for a 10 year operating cycle. Therefore, the total cost for implementing communication improvement will be \$72K.

5. Cost Benefits Analysis

The cost analysis can be traced to the threats scenarios of either data access or physical access. The cost of implementing the data access is linear to its benefit, the benefits of spending \$742K in network security results in a 12.7 percent improvement in probability of detection.

However, for physical access control and the linked response plan, there are multiple factors to examine. Given the costs required to implement various security alternatives that we analyzed, the cost benefit analysis was done to determine the cost efficiency of various alternatives that was modeled previously. The results are plotted in Figure 137. The shape of the graph highlights the correlation of increased performance (Probability of interdiction) with increasing cost. On the lower left corner, it shows the cost and the performance of the current existing system - \$0 cost with performance ~ 0.121. On the other spectrum, it reflects the theoretical maximum probability of interdiction of ~ 0.65 at the cost of nearly \$3.8 million over a ten year period. In terms of cost benefit, this represents a performance gain of 441 percent for a cost of \$4 million. However, if cost is an independent variable that needs to be minimized, then the most insightful point on the graph is the mid-point dip, with the corresponding performance of

0.356 and at a cost of \$732K. Similarly, this result illustrates the performance gain of 194 percent for an increase of \$732K, a more cost efficient solution compared to the theoretical maximum performance solution.

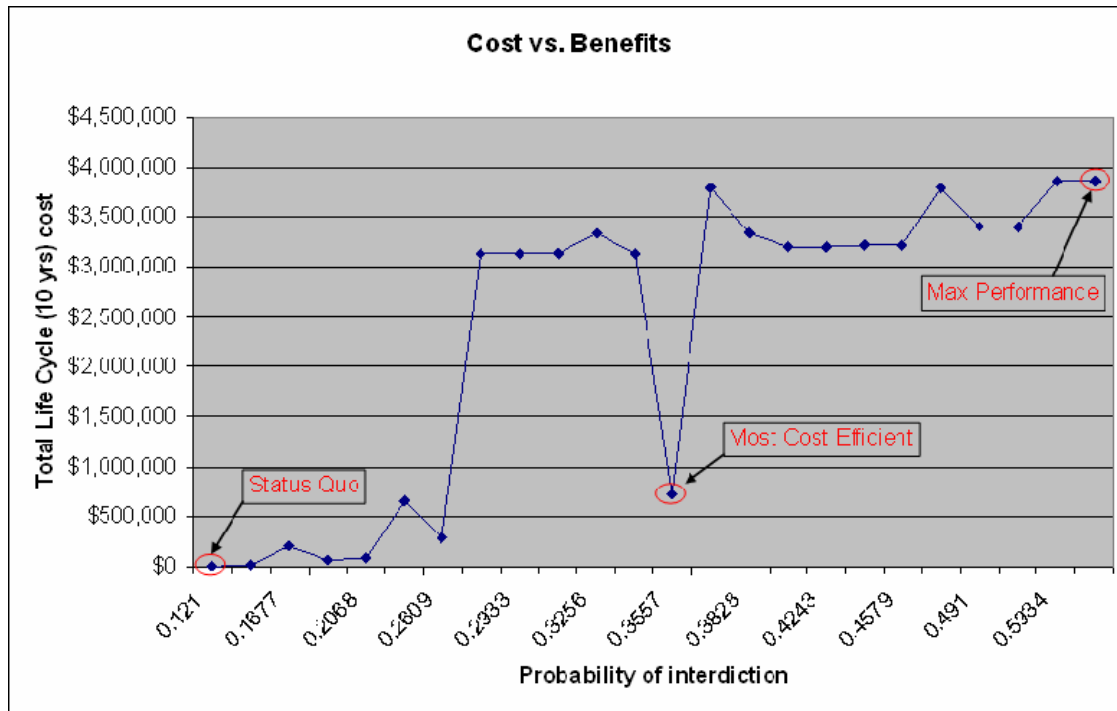


Figure 137. Cost Comparison of All Alternatives Analyzed

In addition to the economic cost of the alternatives, other intangible costs of implementing the proposed solutions are also analyzed. Specifically, the primary question of minimizing operational impact was examined via the EXTEND model. Using queuing theory analysis, delay time and queue length were analyzed and the results are presented in Figure 138. The EXTEND model examined two arrival times that would be submitted to the access control process; in the morning when the workers arrived for the day, and when the workers are returning from lunch. It was determined that the morning rush hour was more critical due to the high density of workers arriving in a short period of time. Nevertheless, the model showed that even for the most stringent security implementation of scanning and random searches would only add at most approximately two minutes to

the required time for employee check in, as compared to the 15 seconds that is currently required for each employee to scan ID badges and transit through the turnstile.

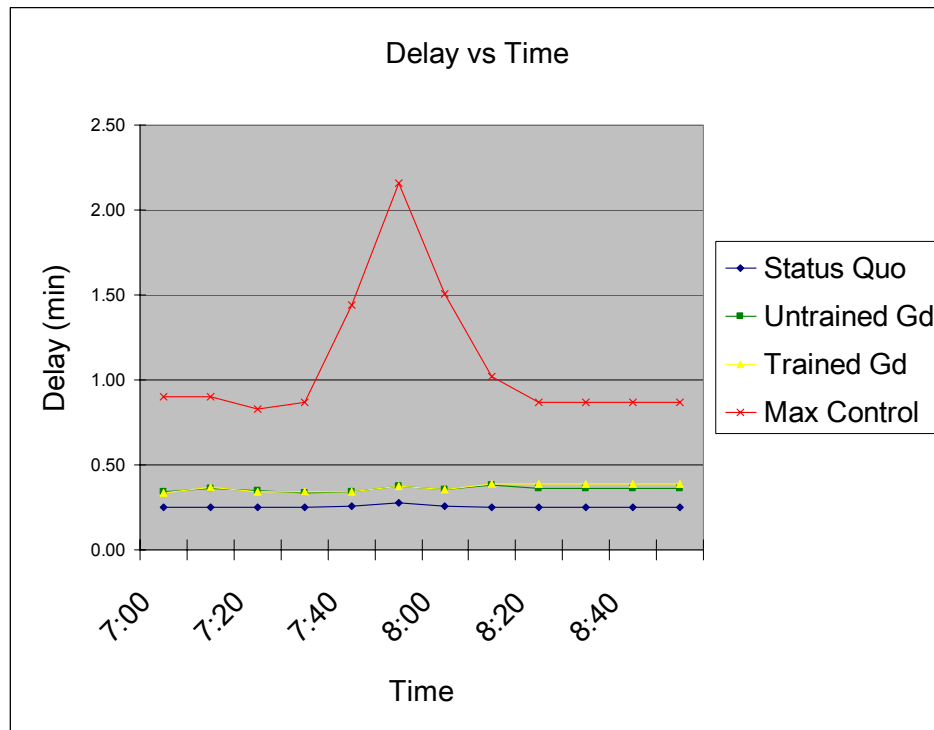


Figure 138. Time Comparison of All Alternatives Analyzed

VI. CONCLUSIONS AND RECOMMENDATIONS

A. TERRESTRIAL THREATS GROUP

1. Conclusions and Recommendations

After the completion of this study, the TTG reached several conclusions. The TTG first noted that perimeter security requirements differ significantly among ports. The likelihood of an attack is a function of geography, potential economic impact, and potential political ramifications. Stakeholders need to determine if their port facilities require improvements in their perimeter and gate security to ensure adequate protection.

The TTG concluded that it is useless for a port to harden its gates without first hardening its perimeter fencing. This conclusion is consistent with United States Coast Guard's recommendations as outlined in the June 2005 Port Security Assessment Best Practices Bulletin [41]. Based on the TTG's cost estimations, the TTG recommends that the port should attach steel reinforced concrete blocks to the base of its preexisting chain link fencing to harden its fences. Implementing concrete blocks would likely have the same effectiveness of implementing a concrete or brick fence but at one twentieth the cost.

After hardening the fencing, the TTG recommends implementing a gate security barrier to stop unauthorized vehicles from entering the terminal. Based on the results of the TTG's modeling, simulation, and cost benefit analysis, the TTG recommends that the terminal implement either spike strips or pop-up barriers but not an armed guard. The implementation of spikes strips costs approximately one-half the cost of implementing pop-up barriers, but provides only one-half the performance. An armed guard should not be implemented because its costs are greater and performance is less than that of spike strips. For optimal performance, the TTG recommends that the port terminal implement pop-up barriers with a set of staggered concrete blocks just before the barrier with a distance of 300 feet or more between the guard house and the pop-up barriers.

2. Areas of Future Study

The TTG recommends that further study be conducted in the areas of gate security and container screening. Further study would be useful in determining effectiveness and impact on commerce as a result of increased screening at the gate for inbound trucks. This study would help stakeholders determine if they should implement additional measures at the truck screening gate. The TTG also recommends that further work be conducted to determine effectiveness and impact on commerce that would result from implementing various types of additional screening from imported containers. Work is currently being done in this area at a classified level by Sandia National Laboratories.

B. REGIONAL SEABORNE THREATS GROUP

1. Conclusions and Recommendations

The RSTG discovered that a layered defense is required in the San Francisco Bay to provide security for the Port of Oakland. The present system is inadequate to support port security in a post 9/11 environment. The RSTG recommends:

- Current Configuration
- USV
- Two X-Band Radar Stations
- Two Thermal Vision Sentry II

The solution that maximizes effectiveness, while minimizing cost is:

- Current Configuration
- USV
- Two X-Band Radar Stations

The effective solution that minimized cost was not chosen because the utility of Thermal Vision Sentry II EO sensors was deemed valuable. The removal or replacement of USVs is a means to reduce cost; however, the RSTG believes that the role of the USV is important and should remain to provide a technological advantage against the threat. Overall, the cost of detecting a terrorist threat is a small fraction of the total cost associated with psychological and reconstruction costs, which could result from a successful terrorist attack. The decision is the stakeholder's who have the option of appropriating more money or opting for a less expensive system configuration.

In addition to a layered defense of sensors, a data fusion center in which the sensor inputs are received and disseminated to the appropriate authorities is needed. In the case of the Port of Oakland, this data fusion center could be located on Yerba Buena Island where there already exists a VTS facility. Another option is Coast Guard Island where the COP may be relayed to the FSO/PSO at the Port of Oakland's premises. This would provide an increased situational awareness which is the key to port security.

Current commercial market systems designed for detecting, tracking, maintaining, and engaging potential terrorist threats can accommodate the sensor and data fusion requirements. Examples of these are: Northrop Grumman's "Hawkeye," Raytheon's "Project Athena," and L3's "HarborGuard." Attached in Appendix J is a test and evaluation test plan that PSS12 constructed for the HarborGuard system.

The ability to have an open architecture sensor infrastructure is also an extremely important aspect to consider. The implementation of USV, X-band radar, and EO sensor capabilities increases awareness of a terrorist threat and provides a better chance of prevention.

2. Areas of Future Study

There still remain unresolved questions that can be examined for future studies. The time constraint prevented the RSTG from addressing all regional threats issues related to port security. The RSTG determined other threats in needs analysis, which were not analyzed. Engagement was another aspect which RSTG did not determine. This aspect would consider the distance at which the threat is discovered and the range needed for engagement. With respect to sensors, the RSTG did not look into a single sensor capable of monitoring multiple small crafts. Overall, the RSTG addressed only a portion of the many facets in dealing with port security against local waterborne threats, opening many areas for future consideration.

C. SOURCE SEABORNE THREATS GROUP

1. Conclusions and Recommendations

The continued joint development of policies to police port security at source ports by world leaders is crucial in the ability to provide safe passage of commerce in the global market. The incorporation of new smart containers, protocol, sensor, and container handling technology into port facilities is an ongoing process that will demand an enormous amount of world resources to implement effectively.

Accurate active scanning equipment to quickly analyze the contents of a container and to determine a threat level associated with that container is an area of study that will demand continual rapid development to increase the security of our ports, ships, and commerce. Fixed and portable scanning equipment that has a high accuracy and low false alarm rate will be required. Reliable, accurate, and cost effective sensors to monitor containers in transit will reduce the amount of time and resources needed to re-inspect containers that have already been inspected at source ports.

The ability of a port that handles high volumes of containers, through the transshipment process, railway, or vehicles, is limited by time, money, and technological constraints to provide a 100 percent safe guarantee that all containers passing through its ports are free of undesired cargoes. The work by the SSTG revealed that a higher probability of detection will come at a cost of higher false alarm rates and therefore will pose a penalty to the productivity of the port measured in its ability to handle containers. The most technologically advanced sensors with a high probability of detection and a low false rate will still generate a significant number of false alarms every day in a port that handles millions of containers per year. The amount of time and money that is required to handle all of these false alarms and to also inspect the randomly targeted containers is a large drain on the port resources. The SSTG Extend model flexibility allows different type of ports and sensor configurations to be represented. The port that the SSTG modeled was a port with high container volume with 95 percent of that volume being generated through transshipment. The alternative that provided the best solution for our MOPs independent of weighting levels for each MOP was the high performance solution. Therefore, the SSTG recommendation for a port with high transshipment volume is to at

a minimum pursue the best crane spreader sensor technology, so that all of the containers can be loaded onto outgoing ships while having the contents scanned simultaneously for undesired cargoes. In addition, the number of inspection teams located at each port needs to be sufficient in size to handle the large volume of containers that will need to be inspected due to false alarms and randomly targeted inspection. The type of sensors, training, and efficient use of port facilities will be instrumental in minimizing the amount of time to inspect and handle containers that need to be inspected is critical in minimizing the disruptions to port operations and commerce. The inspection teams cannot be overlooked as our model demonstrated that the ability to inspect containers effectively and efficiently is a chokepoint in productivity.

2. Areas of Future Study

The SSTG developed several scenarios in earlier sections of this report that were not explored due to the time constraint involved with the generation of this report. The rapid development of new and existing technologies provides a breeding ground for the terrorists to explore new avenues of targeting their enemies. Unmanned aerial vehicles are an example of new technology that has become increasingly available to a wider sector of the world market. Private businesses can mass produce the technology and make it affordable and accessible to main stream terrorists. A feasibility study or analysis of a terrorist attack by an UAV, either by plane or helicopter, on a cargo ship in transit needs to be undertaken. In addition, new methods, procedures, and technology studies need to be considered to enhance ATS ability to identify containers that are possible threats.

The vulnerability of the transshipment process is an area of port security that has not been fully studied or addressed. The port of Singapore is the world's busiest port handling in excess of 23 million TEUs annually and over 90 percent of the containers handled are through the transshipment process. Areas of further study would include how a port can effectively handle containers coming from a non-secure port with minimal facilities, procedures, and equipment to identify undesired cargo into a known secure port that delivers cargo all over the world.

The co-location of commercial shipping hubs with military installations in densely populated areas pose a considerable threat to the economic and defense capabilities of cities and civilian populations located in those areas. The port of Norfolk, which is the 3rd busiest seaport on the east coast of the United States, is representative of such a location. The world's largest navy base is co-located with a busy seaport and local shipyards in a densely populated area. The sinking of a large cargo ship over the Hampton Roads Bridge Tunnel during Christmas time when there are four Nimitz class carriers in port with two other carriers in Newport News Shipyard would be disastrous. The economic impact coupled with the inability to move the countries most valuable Navy assets out of port could be an area of study that needs to be addressed.

The SSTG developed and used an Extend model to draw conclusions on the probability of detection of containers with undesired cargo. The model could be greatly enhanced by studies in how to effectively model real world sensors and the interaction between multiple sensors. The addition of a highly realistic sensor bank could increase the credibility of the studies already completed. In addition, the study in how port facilities are built to yield enormous gains in productivity and efficiency if the facility was designed with a focus on workflow processes, security and safety needs, and setup that could reduce the amount of time that inspection teams would need to inspect suspect containers, and to maximize the number of containers that could be handled per day with minimal resources.

D. INTERNAL PERSONNEL THREATS GROUP

1. Conclusions and Recommendations

The analysis showed that there was a performance benefit to every security option that was analyzed. Given the probability of interdiction of 12 percent for physical access, and 81 percent for catching a rogue employee accessing unauthorized data, both the threats and the consequences of these events are high enough to warrant implementing all the security measures that were analyzed. Specifically, the Max Alternative for physical control access with an upgraded communication system for the security personnel and the

two factor authentication for network security are modeled to increase the likelihood of catching internal employees in the act by more than a factor of four.

2. Areas of Future Study

The analysis of deterrence, access control, and response mechanisms to insider threats provides the port operator a means to control and contain the potential damages that could be caused by an insider threatening the security of the port. However, it is also important that preventive mechanisms be put in place to allow the port operator to actively monitor any suspicious activities and act on them before they become threats. Such preventive mechanism could be of the form of pattern analysis for identification of abnormal behaviors. Research has been done on data mining techniques for misuse detection and anomaly detection, which aim at constructing models to differentiate intrusive and other abnormal behavior from normal behaviors. Techniques current being explored includes statistical modeling, temporal sequence learning, neural network, and genetic algorithms. However, key challenges exist in the form of large data sizes, high dimensionality, the temporal and skewed nature of data, and the requirement for extensive data processing. Existing projects include the MINDS project done by Army High Performance Computing Research Center in University of Minnesota, which attempts to build an anomaly detection system using association pattern analysis. Future work could be done to look into such research which will provide insight into potential areas of focus for implementation of a proactive pattern analysis system to compliment the access, control and response systems.

E. PORT SECURITY STRATEGY BEYOND 2012

The original tasking of the PSS12, from the Wayne E Meyer Institute of Systems Engineering, was to improve port security measures for U.S. ports and Force Protection options for U.S. forces in U.S. and foreign ports. After conducting preliminary research and receiving input from the various stakeholders, PSS12 concluded the best option to protect U.S. forces and commercial vessels while in-port was to secure the port facilities. To secure the port facilities, PSS12 examined the potential avenues from which a threat may originate and modeled options to defeat the threat.

By conducting this study in the previous manner, it was evident that Port Security is a disjointed problem. PSS12 limited the alternatives by specifying that the alternatives must be able to be implemented by 2012. When dividing into the four sub-groups to address the different aspects from which a threat may originate, PSS12 established geographical and jurisdictional boundaries between the sub-groups to avoid duplication of efforts. The result of the total effort was four distinct systems that addressed threats from the four examined avenues.

An additional portion of the initial tasking of PSS12 was to design a system of systems that addressed the issue of port security. Due to the disjointed problem of port security, there was not a single system that addressed all the avenues from which threats may come. Threats to a port facility originate from various locations, display different characteristics that enable detection, and operate in different environments (i.e. land or sea).

The relatively short timeframe given to examine the problem of port security did not enable PSS12 to adequately address the issue of integration of these systems. PSS12 presented different system alternatives to address the diverse threats. One challenge to the integration of such systems requires the stakeholder to choose which systems are desired based on his specific need. The different alternatives presented within each sub-group have different hardware and software requirements, maintenance schedules, and operation and training requirements. Acquiring a stakeholder decision was beyond the scope of this project.

However, an initial discussion among the members of PSS12 yielded that one option that addresses the problem of integration of the systems is the establishment of a command center. The purpose of such would be to create a central location, staffed with trained personnel, to which the information from the various sensors is relayed. The information would originate from the sensors of the different systems the stakeholder decided to implement.

With the establishment of a command center, the issue of data fusion arises. The different agencies, whose efforts collectively provide port security, have different

jurisdictions, organizational structures, and funding. With these agencies, a serious coordination problem becomes evident. The information received from the agencies must be rapidly received, displayed, interpreted and responded to in order for the system to be effective. From conducting this study, PSS12 recognized that the fusion of data is a critical issue that needs to be addressed. Data fusion was beyond the scope of this project; however, is an area where future study is required.

A second function of the command center would be to coordinate the appropriate response to any incident. This conceptual command center would require hardware and software to process information in order to provide a common operational picture for the operators required to make quick and appropriate decision. Communications links would be vital as well because some of the alternative presented require human detection and response. Along with the information processing requirement, the communications requirements for the selected alternatives differ with the alternatives that are chosen for implementation. The types of systems the stakeholder implements will directly determine the robustness of this conceptual command center.

The command center is one possible alternative for addressing the problem of integration of the systems. PSS12 was not able to fully examine the systems integration issue in order to adequately address the problems of threat detection and intervention. The integration of such systems remains as a possible study regarding the problem of port security.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A: TTG MODELS

Model Alternatives (Defensive Measures, Distances, Concrete Block Positions)

Trial	Barrier Type	Security Zone Distance (ft)	Blocks/position	Trial	Barrier Type	Security Zone Distance (ft)	Blocks/position
1	Status Quo	900	No Blocks	31	Status Quo	700	No Blocks
2	Pop-Up Barrier	900	No Blocks	32	Pop-Up Barrier	700	No Blocks
3	Spike Strips	900	No Blocks	33	Spike Strips	700	No Blocks
4	Armed Guard	900	No Blocks	34	Armed Guard	700	No Blocks
5	Pop-Up Barrier	900	Gate	35	Pop-Up Barrier	700	Gate
6	Spike Strips	900	Gate	36	Spike Strips	700	Gate
7	Armed Guard	900	Gate	37	Armed Guard	700	Gate
8	Pop-Up Barrier	900	Barrier	38	Pop-Up Barrier	700	Barrier
9	Spike Strips	900	Barrier	39	Spike Strips	700	Barrier
10	Armed Guard	900	Barrier	40	Armed Guard	700	Barrier
11	Status Quo	500	No Blocks	41	Status Quo	300	No Blocks
12	Pop-Up Barrier	500	No Blocks	42	Pop-Up Barrier	300	No Blocks
13	Spike Strips	500	No Blocks	43	Spike Strips	300	No Blocks
14	Armed Guard	500	No Blocks	44	Armed Guard	300	No Blocks
15	Pop-Up Barrier	500	Gate	45	Pop-Up Barrier	300	Gate
16	Spike Strips	500	Gate	46	Spike Strips	300	Gate
17	Armed Guard	500	Gate	47	Armed Guard	300	Gate
18	Pop-Up Barrier	500	Barrier	48	Pop-Up Barrier	300	Barrier
19	Spike Strips	500	Barrier	49	Spike Strips	300	Barrier
20	Armed Guard	500	Barrier	50	Armed Guard	300	Barrier
21	Status Quo	100	No Blocks				
22	Pop-Up Barrier	100	No Blocks				
23	Spike Strips	100	No Blocks				
24	Armed Guard	100	No Blocks				
25	Pop-Up Barrier	100	Gate				
26	Spike Strips	100	Gate				
27	Armed Guard	100	Gate				
28	Pop-Up Barrier	100	Barrier				
29	Spike Strips	100	Barrier				
30	Armed Guard	100	Barrier				

Table A1: TTG Model Alternatives

Model Inputs (Delays, Reliability, Effectiveness)

Trial	Replication Description	Obstacle Delay	sec zone delay	report delay	barrier delay	reliability (%)	effectiveness (%)
1	Status Quo-900'-No Blocks	0	19.6, 24.4, 29.3	0	0	95	0
2	Pop-Up Barrier-900'-No Blocks	0	19.6, 24.4, 29.3	1, 3, 6	1, 2, 5	95	90
3	Spike Strips-900'-No Blocks	0	19.6, 24.4, 29.3	1, 3, 6	1, 1.5, 2	95	48
4	Armed Guard-900'-No Blocks	0	19.6, 24.4, 29.3	2,3,5	5, 15, 30	75	10
5	Pop-Up Barrier-900'-Blocks@Gate	0	22.7, 28.4, 34.1	1, 3, 6	1, 2, 5	95	91
6	Spike Strips-900'-Blocks@Gate	0	22.7, 28.4, 34.1	1, 3, 6	1, 1.5, 2	95	50
7	Armed Guard-900'-Blocks@Gate	0	22.7, 28.4, 34.1	2,3,5	5, 15, 30	75	12
8	Pop-Up Barrier-900'-Blocks@Barrier	5.5,6.8,8.2	18, 22.4, 27	1, 3, 6	1, 2, 5	95	100
9	Spike Strips-900'-Blocks@Barrier	5.5,6.8,8.2	18, 22.4, 27	1, 3, 6	1, 1.5, 2	95	30
10	Armed Guard-900'-Blocks@Barrier	5.5,6.8,8.2	18, 22.4, 27	2,3,5	5, 15, 30	75	14
11	Status Quo-500'-No Blocks	0	12.6, 15.8, 18.9	0	0	95	0
12	Pop-Up Barrier-500'-No Blocks	0	12.6, 15.8, 18.9	1, 3, 6	1, 2, 5	95	94
13	Spike Strips-500'-No Blocks	0	12.6, 15.8, 18.9	1, 3, 6	1, 1.5, 2	95	40
14	Armed Guard-500'-No Blocks	0	12.6, 15.8, 18.9	2,3,5	5, 15, 30	75	38
15	Pop-Up Barrier-500'-Blocks@Gate	0	15.3, 19.1, 22.9	1, 3, 6	1, 2, 5	95	95
16	Spike Strips-500'-Blocks@Gate	0	15.3, 19.1, 22.9	1, 3, 6	1, 1.5, 2	95	42
17	Armed Guard-500'-Blocks@Gate	0	15.3, 19.1, 22.9	2,3,5	5, 15, 30	75	40
18	Pop-Up Barrier-500'-Blocks@Barrier	5.5,6.8,8.2	10.6, 13.3, 15.9	1, 3, 6	1, 2, 5	95	100
19	Spike Strips-500'-Blocks@Barrier	5.5,6.8,8.2	10.6, 13.3, 15.9	1, 3, 6	1, 1.5, 2	95	30
20	Armed Guard-500'-Blocks@Barrier	5.5,6.8,8.2	10.6, 13.3, 15.9	2,3,5	5, 15, 30	75	42
21	Status Quo-100'-No Blocks	0	3.2, 4, 4.9	0	0	95	0
22	Pop-Up Barrier-100'-No Blocks	0	3.2, 4, 4.9	1, 3, 6	1, 2, 5	95	97
23	Spike Strips-100'-No Blocks	0	3.2, 4, 4.9	1, 3, 6	1, 1.5, 2	95	32
24	Armed Guard-100'-No Blocks	0	3.2, 4, 4.9	2,3,5	5, 15, 30	75	10
25	Pop-Up Barrier-100'-Blocks@Gate	0	4.4 5.5, 6.6	1, 3, 6	1, 2, 5	95	98
26	Spike Strips-100'-Blocks@Gate	0	4.4 5.5, 6.6	1, 3, 6	1, 1.5, 2	95	33
27	Armed Guard-100'-Blocks@Gate	0	4.4 5.5, 6.6	2,3,5	5, 15, 30	75	12
28	Pop-Up Barrier-100'-Blocks@Barrier	5.5,6.8,8.2	0	1, 3, 6	1, 2, 5	95	100
29	Spike Strips-100'-Blocks@Barrier	5.5,6.8,8.2	0	1, 3, 6	1, 1.5, 2	95	30
30	Armed Guard-100'-Blocks@Barrier	5.5,6.8,8.2	0	2,3,5	5, 15, 30	75	12
31	Status Quo-700'-No Blocks	0	16.3, 20.4, 24.4	0	0	95	0
32	Pop-Up Barrier-700'-No Blocks	0	16.3, 20.4, 24.4	1, 3, 6	1, 2, 5	95	92
33	Spike Strips-700'-No Blocks	0	16.3, 20.4, 24.4	1, 3, 6	1, 1.5, 2	95	44
34	Armed Guard-700'-No Blocks	0	16.3, 20.4, 24.4	2,3,5	5, 15, 30	75	22
35	Pop-Up Barrier-700'-Blocks@Gate	0	19.2, 24, 28.8	1, 3, 6	1, 2, 5	95	93
36	Spike Strips-700'-Blocks@Gate	0	19.2, 24, 28.8	1, 3, 6	1, 1.5, 2	95	46
37	Armed Guard-700'-Blocks@Gate	0	19.2, 24, 28.8	2,3,5	5, 15, 30	75	20
38	Pop-Up Barrier-700'-Blocks@Barrier	5.5,6.8,8.2	14.5, 18.1, 21.8	1, 3, 6	1, 2, 5	95	100
39	Spike Strips-700'-Blocks@Barrier	5.5,6.8,8.2	14.5, 18.1, 21.8	1, 3, 6	1, 1.5, 2	95	30
40	Armed Guard-700'-Blocks@Barrier	5.5,6.8,8.2	14.5, 18.1, 21.8	2,3,5	5, 15, 30	75	22
41	Status Quo-300'-No Blocks	0	8.4, 10.5, 12.6	0	0	95	0
42	Pop-Up Barrier-300'-No Blocks	0	8.4, 10.5, 12.6	1, 3, 6	1, 2, 5	95	95
43	Spike Strips-300'-No Blocks	0	8.4, 10.5, 12.6	1, 3, 6	1, 1.5, 2	95	36
44	Armed Guard-300'-No Blocks	0	8.4, 10.5, 12.6	2,3,5	5, 15, 30	75	22
45	Pop-Up Barrier-300'-Blocks@Gate	0	10.6, 13.2, 15.9	1, 3, 6	1, 2, 5	95	96
46	Spike Strips-300'-Blocks@Gate	0	10.6, 13.2, 15.9	1, 3, 6	1, 1.5, 2	95	38
47	Armed Guard-300'-Blocks@Gate	0	10.6, 13.2, 15.9	2,3,5	5, 15, 30	75	20
48	Pop-Up Barrier-300'-Blocks@Barrier	5.5,6.8,8.2	6, 7.5, 9	1, 3, 6	1, 2, 5	95	100
49	Spike Strips-300'-Blocks@Barrier	5.5,6.8,8.2	6, 7.5, 9	1, 3, 6	1, 1.5, 2	95	30
50	Armed Guard-300'-Blocks@Barrier	5.5,6.8,8.2	6, 7.5, 9	2,3,5	5, 15, 30	75	22

Table A2: TTG Model Inputs

APPENDIX B: TTG MODELING RESULTS

Data by Distance

Configuration	Effectiveness
SQ-100	0
PB-CB(N)-100	0.06816609
SS-CB(N)-100	0.075951557
AG-CB(N)-100	0
PB-CB(G)-100	0.348673587
SS-CB(G)-100	0.224077278
AG-CB(G)-100	0
PB-CB(B)-100	0.682497116
SS-CB(B)-100	0.269232987
AG-CB(B)-100	0
SQ-300	0
PB-CB(N)-300	0.898442907
SS-CB(N)-300	0.34106113
AG-CB(N)-300	0.003690888
PB-CB(G)-300	0.911418685
SS-CB(G)-300	0.360178777
AG-CB(G)-300	0.015599769
PB-CB(B)-300	0.950374856
SS-CB(B)-300	0.285207612
AG-CB(B)-300	0.024798155
SQ-500	0
PB-CB(N)-500	0.89310842
SS-CB(N)-500	0.379527105
AG-CB(N)-500	0.063754325
PB-CB(G)-500	0.931430219
SS-CB(G)-500	0.407814302
AG-CB(G)-500	0.13638985
PB-CB(B)-500	0.950374856
SS-CB(B)-500	0.285207612
AG-CB(B)-500	0.16349481
SQ-700	0
PB-CB(N)-700	0.873933103
SS-CB(N)-700	0.416998633
AG-CB(N)-700	0.088696655
PB-CB(G)-700	0.882958478
SS-CB(G)-700	0.436908881
AG-CB(G)-700	0.113465975
PB-CB(B)-700	0.950374856
SS-CB(B)-700	0.285207612
AG-CB(B)-700	0.133419839
SQ-900	0
PB-CB(N)-900	0.855305652
SS-CB(N)-900	0.455161476
AG-CB(N)-900	0.058044983
PB-CB(G)-900	0.864446367
SS-CB(G)-900	0.474480969
AG-CB(G)-900	0.083102653
PB-CB(B)-900	0.950374856
SS-CB(B)-900	0.2838812
AG-CB(B)-900	0.100346021

Data By Barrier Configuration

Configuration	Effectiveness
SQ-100	0
SQ-300	0
SQ-500	0
SQ-700	0
SQ-900	0
AG-CB(B)-100	0
AG-CB(B)-300	0.024798155
AG-CB(B)-500	0.16349481
AG-CB(B)-700	0.133419839
AG-CB(B)-900	0.100346021
AG-CB(G)-100	0
AG-CB(G)-300	0.015599769
AG-CB(G)-500	0.13638985
AG-CB(G)-700	0.113465975
AG-CB(G)-900	0.083102653
AG-CB(N)-100	0
AG-CB(N)-300	0.003690888
AG-CB(N)-500	0.063754325
AG-CB(N)-700	0.088696655
AG-CB(N)-900	0.058044983
SS-CB(B)-100	0.269232987
SS-CB(B)-300	0.285207612
SS-CB(B)-500	0.285207612
SS-CB(B)-700	0.285207612
SS-CB(B)-900	0.2838812
SS-CB(G)-100	0.224077278
SS-CB(G)-300	0.360178777
SS-CB(G)-500	0.407814302
SS-CB(G)-700	0.436908881
SS-CB(G)-900	0.474480969
SS-CB(N)-100	0.075951557
SS-CB(N)-300	0.34106113
SS-CB(N)-500	0.379527105
SS-CB(N)-700	0.416998633
SS-CB(N)-900	0.455161476
PB-CB(B)-100	0.682497116
PB-CB(B)-300	0.950374856
PB-CB(B)-500	0.950374856
PB-CB(B)-700	0.950374856
PB-CB(B)-900	0.950374856
PB-CB(G)-100	0.348673587
PB-CB(G)-300	0.911418685
PB-CB(G)-500	0.931430219
PB-CB(G)-700	0.882958478
PB-CB(G)-900	0.864446367
PB-CB(N)-100	0.06816609
PB-CB(N)-300	0.898442907
PB-CB(N)-500	0.89310842
PB-CB(N)-700	0.873933103
PB-CB(N)-900	0.855305652

Data By Effectiveness

Configuration	Effectiveness
PB-CB(B)-900	0.950374856
PB-CB(B)-700	0.950374856
PB-CB(B)-500	0.950374856
PB-CB(B)-300	0.950374856
PB-CB(G)-500	0.931430219
PB-CB(G)-300	0.911418685
PB-CB(N)-300	0.898442907
PB-CB(N)-500	0.89310842
PB-CB(G)-700	0.882958478
PB-CB(N)-700	0.873933103
PB-CB(G)-900	0.864446367
PB-CB(N)-900	0.855305652
PB-CB(B)-100	0.682497116
SS-CB(G)-900	0.474480969
SS-CB(N)-900	0.455161476
SS-CB(G)-700	0.436908881
SS-CB(N)-700	0.416998633
SS-CB(G)-500	0.407814302
SS-CB(N)-500	0.379527105
SS-CB(G)-300	0.360178777
PB-CB(G)-100	0.348673587
SS-CB(N)-300	0.34106113
SS-CB(B)-700	0.285207612
SS-CB(B)-300	0.285207612
SS-CB(B)-500	0.285207612
SS-CB(B)-900	0.2838812
SS-CB(B)-100	0.269232987
SS-CB(G)-100	0.224077278
AG-CB(B)-500	0.16349481
AG-CB(G)-500	0.13638985
AG-CB(B)-700	0.133419839
AG-CB(G)-700	0.113465975
AG-CB(B)-900	0.100346021
AG-CB(N)-700	0.088696655
AG-CB(G)-900	0.083102653
SS-CB(N)-100	0.075951557
PB-CB(N)-100	0.06816609
AG-CB(N)-500	0.063754325
AG-CB(N)-900	0.058044983
AG-CB(B)-300	0.024798155
AG-CB(G)-300	0.015599769
AG-CB(N)-300	0.003690888
AG-CB(N)-100	0
AG-CB(G)-100	0
AG-CB(B)-100	0
SQ-900	0
SQ-700	0
SQ-500	0
SQ-300	0
SQ-100	0

Table B1: TTG Simulation Results

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C: TTG LIFE CYCLE COST DSC2000 BARRIER

In its attempt to design a system of systems to protect foreign and domestic ports, PSS12 was tasked to construct reliability and lifecycle cost analysis of one selected alternatives. The alternative that was chosen was the DSC 2000, which is a pop-up barrier system that prevents unauthorized vehicles from infiltrating a port facility by running the gate. The DSC 2000 is sold by the Delta Scientific Corporation and is the currently used at the Ninth Street gate at the Naval Postgraduate School. The proximity of this system provided ample opportunity to correspond with the system operators and designers to provide the information required for such study.

For the purpose of this study, all costs are stated in fiscal year 2007 United States Dollars (USD). From a various phone conversations and emails with Mr. Gregg Hamm, who is the High Security Systems Technician for Delta Scientific Corporation, the cost of procuring the DSC 2000 pop-up barrier system depends on how many pop-up mechanisms are desired. This number directly corresponds to the width of the travel lane that the security personnel wish to impede. Mr. Hamm stated that a travel lane of width of twelve feet, three pop-up barriers are recommended. He further stated that procurement of such a system involves the purchasing of the parts and installation of the system. The purchase of the three pop-up barrier system costs approximately 40 – 45 thousand dollars. Mr. Hamm added that a good rule of thumb for installment cost for these systems is 90-95 percent of the purchase cost bring the total cost for the procurement of this system to approximately 80 – 85 thousand dollars.

The two major components of the DSC 2000 are the pop-up barriers and the hydraulic power unit. The pop up barriers are installed in the vehicle lanes of travel. Their purpose is to impede the vehicle from penetrating into the facility by blocking the travel lane upon activation by the security personnel. These barriers are constructed of heavy metal obstructions that are hydraulically lifted from the roadway to impede vehicle passage. An extended version of the pop-up barrier is shown in Figure C1.

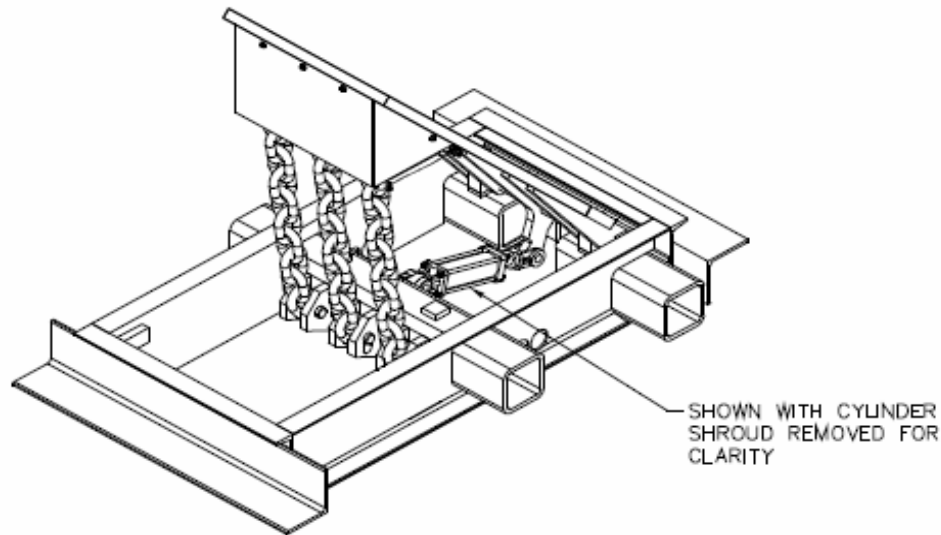


Figure C1. Extended Pop-Up Barrier

In Figure C1, the hydraulic cylinder receives fluid from the system to raise and lower the barrier. The components of this system are not very complex.

The maintenance required for this portion of the system requires greasing the hinges, tightening the bolts as necessary, and maintaining the nitrogen pre-charge of the actuator. These actions are required monthly except for the checking of the nitrogen pre-charge. The checking of the nitrogen pre-charge is directed to be conducted at least every six months according to the Delta Scientific Maintenance Manual for the DSC 2000.

For the purpose of this study, the procurement costs of common tools required for maintenance such as wrenches, screwdrivers and hammers will not be figured into the operating and support costs. The maintenance for the pop-up barrier portion of the DSC 2000 is relatively inexpensive. A simplified version of the pop-up barriers is shown in Figure C2.

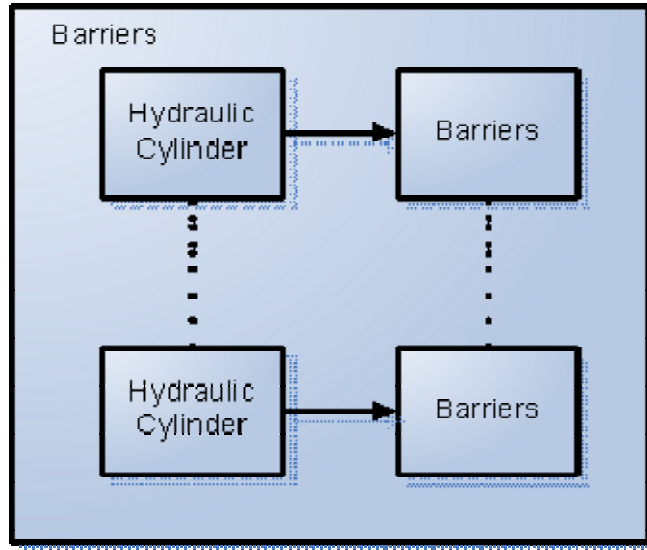


Figure C2. Simplified Diagram of the Barrier System

This pop-up barrier subsystem is not very complex. The only specialized tool required for maintenance is required for checking and maintaining the nitrogen pre-charge on the barrier hydraulic actuators. The Delta Scientific Maintenance Manual recommends purchasing the Delta Charging Kit # 2469-31 for use in this task. The charging kit has a one time cost of \$217.30. Nitrogen is only required in these actuators if it is evident that a leak is present which leads to bigger issues. The hinges and bolts require greasing and tightening at least once every month. From the conduction a market survey, a 40 cubic foot nitrogen cylinder costs approximately \$100.00. Once used, these nitrogen gas cylinders may be recharged at a gas supplier that can range from \$20 to \$40. The grease required to lubricate the system costs from \$4 to \$6 per pound cartridge. Overall, the maintenance of the pop-up barrier system is minimal with most of the cost being the initial procurement of the tools necessary to recharge the cylinder. The initial procurement of these tools sums to \$317.30 with the recurring yearly cost being primarily for the lubricant and nitrogen. Assuming that one nitrogen bottle is used per year and on pound on grease is used each month per pop-up barrier of a three lane system, the annual scheduled maintenance cost for the parts of the system is \$210.00.

The more complex portion of the barrier system is the Hydraulic Power Unit (HPU). The purpose of the HPU is to maintain the primed pressure on several of the systems actuators to enable the system to be deployed in according to the one-half second advertisement. A simplified block diagram of the components of the HPU is shown in Figure C3.

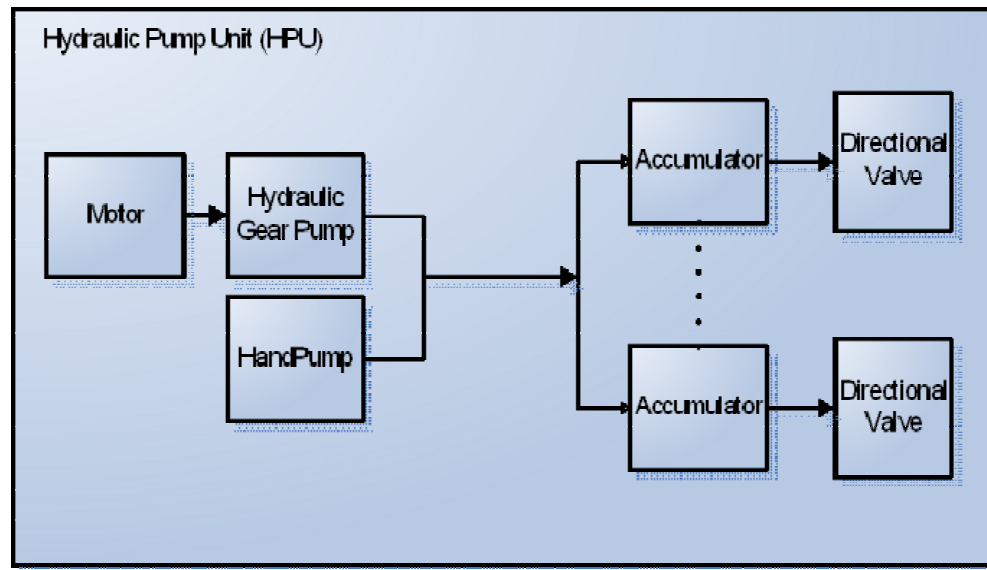


Figure C3. Simplified block Diagram of HPU

The concept of operation for this system in the normal mode is an electric motor drives a hydraulic gear pump. The motor and hydraulic gear pump is connected in parallel with the hand pump. The hand pump provides a method to manually charge the system with hydraulic pressure in case of a motor failure. These pumps pressurize several accumulators which maintain the pressure charge required for the rapid actuation of the barriers. After the accumulators are the directional valves which determines the direction of the hydraulic fluid flow to the pop-up barrier actuators. The pop-up barriers are hydraulically powered up and down and the directional valves are the mechanisms that control the direction of actuation.

The monthly scheduled maintenance directed by the Delta Scientific Manuals for the HPU is not extensive. The monthly scheduled maintenance for the HPU includes changing the hydraulic fluid filter and topping off the hydraulic fluid contained in the

reservoir (if any of these are necessary). The manual recommends changing the hydraulic fluid filter every third month. Mr. Hamm said these oil filters costs approximately \$60.00 each. Changing these oil filters every three months requires four oil filters per year bringing the total yearly cost for the oil filters to \$240.00.

The yearly scheduled maintenance directed by the manual directs a full flush and refill of the hydraulic fluid contained in the HPU. The capacity of the HPU reservoir is 20 gallons for the typical three lane system. The Delaware State Contract procurement Office obtains the required Shell Tellus 46 Hydraulic Fluid for 6.50 per gallon. To fully flush and fill the system would cost an annual amount of \$130.00. The scheduled maintenance parts cost for the HPU would be \$370.00 annually. For the entire system, the cost for the parts would be \$580.00.

Delta Scientific (Delta) estimates the DSC 2000 system can perform its functionality between 15 to 20 years when regular preventive maintenance is conducted according to the recommendations in the manual. Assuming time T is an exponential random variable, the reliability of the system after one year would be between 93.4 and 95.1 percent. There is a generous assumption that most component failures do not affect the performance of the system's stated functionality are not considered as system failures while the system is addressed as one big complex component. In the examination of the system design documents and maintenance guidelines, the critical components affecting the full operational functionality of the barriers system were identified and shown in Table C1. A common system problem highlighted by Delta is the Hydraulic Pump Unit (HPU). The HPU Mean Time Between Failure (MTBF) estimate given by Delta is between 10 to 15 years. The HPU is driven either via electrical or manual methods. With the parallel connectivity driving the HPU, the overall reliability of the HPU is 98.5 percent as shown in Table C2.

Critical Components	MTBF	R _i
Motor	10	0.904837
Motor Switch	15	0.935507
Hydraulic Pump & Reservoir	5	0.818731
Hand pump	20	0.951229
Hose & Fitting	8	0.882497
Accumulator	12	0.920044
Directional Valve	15	0.935507
Hydraulic Cylinder	12	0.920044
Barrier	50	0.980199

Table C1. Reliability of Critical Components of the Barriers System for One Year

Hydraulic Pump Unit	R _i
Electric Hydraulic Pump	0.693041
Hand Pump	0.951229
Overall Reliability of Hydraulic Pump Unit	0.985029

Table C2. Reliability of the Hydraulic Pump Subsystem for One Year

Most of the components MTBF are not available and the estimates for them are based on analogy. Personal experience on similar parts working in various systems such as automobile and helicopter systems were use to give the “best estimate” with large assumptions. The remaining data from Delta is the fitting and hose that requires to be replaced every seven to eight years. This is due to abrasion by the contaminants in the hydraulic fluid and causing wear and tear over prolonged usage. The MTBF and the reliabilities for the components are shown in Table C1.

The HPU, hose and fitting, accumulator, directional valve, hydraulic cylinder and the barrier are treated as connected in a series. The product of the individual reliabilities works out to be 67.5 percent for the overall system reliability. While there is a big contrast between Delta’s estimate and calculated reliabilities, assumptions used were generous and field data are not available to enable higher accuracy in the estimation.

Delta Scientific’s spare parts list for the DSC 2000 is included on the following pages for estimating the cost of components for unscheduled maintenance.

DELTA SCIENTIFIC CORPORATION
 40355 DELTA LANE
 PALMDALE, CALIFORNIA, 91355, USA

PHONE 661-575-1100
 FAX 661-575-1109
 EMAIL info@deltascientific.com

TYPICAL SPARE PARTS LIST DSC2000
DELTA MODEL S DSC2000 PHALANX BARRIERS

ELECTRICAL PARTS

EFFECTIVE May 22, 2007

STK NO.	DESCRIPTION	UNIT COST
2459-10	FUSE, 250 V, 2.5 AMP,	7.75/FIVE
2459-12	FUSE, 250 V, 7.5 AMP,	7.75/FIVE
2459-119	FUSE, 250 V, 3.5 AMP,	7.75/FIVE
2461-25	POWER SUPPLY, 150 WATTS,	332.09
2461-40	BATTERY, 12 VOLT, 7 AMP-HOUR	48.30
2463-01	KEY SWITCH,	21.81
2463-02A	SELECTOR SWITCH,	22.00
2463-03A	EFO, HOODED TOGGLE TYPE,	34.93
2463-06	PUSHBUTTON, N.O. BLACK,	10.15
2463-07	PUSHBUTTON, N.C. RED,	9.98
2463-16	PILOT LIGHT, LED, RED,	14.75
2463-17	PILOT LIGHT, LED, GREEN,	14.75
2463-64	ANNUNCIATOR SIREN,	32.55
2464-165	MOTOR, 5 HP @ 220/3/50,	750.00
2465-01	PRESSURE SWITCH,	198.45
2465-11	LEVEL SWITCH,	90.72
2465-31	LIMIT SWITCH, MAGNETIC,	24.05
2465-42	HEATER, 500 W @ 240 V,	369.46
2465-66	3 PH. POWER MONITOR,	206.78
2467-01	DIRECT. VALVE, DO3, 24 VDC,	308.07
2467-31	EFO VALVE, 24 VDC,	105.84
2531-66	STARTER OVERLOAD, 3.2 – 16 A,	76.41
2531-108	MOTOR STARTER,	139.55
2531-110	DISCONNECT SWITCH, 30 AMP,	187.50
2534-68	TIMER RELAY TRIM POT,	8.25
2534-69	TIMER RELAY, 24 VDC,	116.66
90605	BARRIER CONTROL CARD,	500.00
IN5404	DIODE	2.00
1/4W1.2K	RESISTOR	2.00
MANUAL	OWNERS MANUAL	SERIAL NUMBER 6528 65.00

PRICES SUBJECT TO CHANGE WITHOUT NOTICE.

PRICES ARE NET 30 DAYS TO APPROVED ACCOUNTS, FOB PALMDALE, CALIFORNIA.
SEE ORDERING INSTRUCTIONS TO ASSURE THAT PROPER PARTS ARE ORDERED.

Copyright 2006 Delta Scientific Corporation
 All Rights Reserved

Page 1 of 2
 Document Spare Parts

DELTA SCIENTIFIC CORPORATION
 40355 DELTA LANE
 PALMDALE, CALIFORNIA, 91355, USA

PHONE 661-575-1100
 FAX 661-575-1109
 EMAIL info@deltascientific.com

TYPICAL SPARE PARTS LIST DSC2000
DELTA MODEL S DSC2000 PHALANX BARRIERS

MECHANICAL PARTS

EFFECTIVE April 28, 2006

STK NO.	DESCRIPTION	UNIT COST
1501-04	CAP SCREW, 1/2"-20 X 2"LG,	2.78
2464-32	MOTOR/PUMP ADAPTER,	140.00
2464-52	MOTOR HALF COUPLING,	23.66
2464-53	PUMP HALF COUPLING,	23.66
2464-61	COUPLING SPIDER,	11.41
2465-05	PRESSURE RELIEF VALVE,	81.66
2465-21	PRESSURE GAGE, 0-3000 PSIG,	38.33
2465-22	LEVEL GAGE, 10",	42.11
2465-23	GAGE SNUBBER,	21.07
2465-91	TOOL KIT IN TOOL BOX,	231.25
2466-03	1/2" FLOW CONTROL VALVE,	80.33
2466-11	1/4" NEEDLE VALVE,	48.27
2466-12	3/8" NEEDLE VALVE,	58.63
2466-33B	1/2" BALL VALVE, BRONZE,	23.94
2466-66	1/2" CHECK VALVE, INLINE,	88.00
2468-08	HYDR. CYLINDER, 2.5" X 6",	217.32
2468-13	HYD CYLINDER SEAL KIT, 2.5",	25.73
2469-31	ACCUM CHARGE KIT,	181.04
2469-51	ACCUM CHARGE BOTTLE,	220.50
2469-72	ACCUMULATOR, 5.0 GALLON,	1,221.00
2469-81	ACCUM REBUILD KIT, 6 INCH,	157.43
2470-12	FILTER ELEMENT, TANK TOP,	53.90
2470-41	SUCTION STRAINER,	20.83
2470-43	FILLER BREATHER,	23.38
2471-21	HAND PUMP, COMPLETE,	359.35
2471-31	HAND PUMP, SEAL KIT,	47.25
2512-4-FT	HOSE ASSY, 1/4" X xx FT LG,	\$ 3.43/FT + 23.69
2512-6-FT	HOSE ASSY, 3/8" X xx FT LG,	\$ 3.71/FT + 24.72
2512-8-FT	HOSE ASSY, 1/2" X xx FT LG,	\$ 4.31/FT + 24.75
2739-010	BEARING BLOCK, 4 BOLT,	59.50
2739-02G	BEARING BLOCK BUSHING,	17.14
2739-05G	CYLINDER HANGER BUSHING,	11.82

PRICES SUBJECT TO CHANGE WITHOUT NOTICE.

PRICES ARE NET 30 DAYS TO APPROVED ACCOUNTS, FOB PALMDALE, CALIFORNIA.

SEE ORDERING INSTRUCTIONS TO ASSURE THAT PROPER PARTS ARE ORDERED.

APPENDIX D: TTG COST BENEFIT ANALYSIS

Configuration	Effectiveness	Annual Cost (USD)	Configuration	Effectiveness	Annual Cost (USD)
SQ-100	0	0	PB-CB(B)-900	0.950374856	37100
SQ-300	0	0	PB-CB(B)-700	0.950374856	37100
SQ-500	0	0	PB-CB(B)-500	0.950374856	37100
SQ-700	0	0	PB-CB(B)-300	0.950374856	37100
SQ-900	0	0	PB-CB(G)-500	0.931430219	37100
SS-CB(N)-100	0.075951557	15566	PB-CB(G)-300	0.911418685	37100
SS-CB(N)-300	0.34106113	15566	PB-CB(N)-300	0.898442907	37010
SS-CB(N)-500	0.379527105	15566	PB-CB(N)-500	0.89310842	37010
SS-CB(N)-700	0.416998633	15566	PB-CB(G)-700	0.882958478	37100
SS-CB(N)-900	0.455161476	15566	PB-CB(N)-700	0.873933103	37010
SS-CB(G)-100	0.224077278	15656	PB-CB(G)-900	0.864446367	37100
SS-CB(B)-100	0.269232987	15656	PB-CB(N)-900	0.855305652	37010
SS-CB(B)-300	0.2838812	15656	PB-CB(B)-100	0.682497116	37100
SS-CB(B)-500	0.285207612	15656	SS-CB(G)-900	0.474480969	15656
SS-CB(B)-700	0.285207612	15656	SS-CB(N)-900	0.455161476	15656
SS-CB(B)-900	0.285207612	15656	SS-CB(G)-700	0.436908881	15656
PB-CB(G)-100	0.348673587	15656	SS-CB(N)-700	0.416998633	15566
SS-CB(G)-300	0.360178777	15656	SS-CB(G)-500	0.407814302	15656
SS-CB(G)-500	0.407814302	15656	SS-CB(N)-500	0.379527105	15566
SS-CB(G)-700	0.436908881	15656	SS-CB(G)-300	0.360178777	15656
SS-CB(G)-900	0.474480969	15656	PB-CB(G)-100	0.348673587	15656
AG-CB(N)-100	0	36275	SS-CB(N)-300	0.34106113	15566
AG-CB(N)-300	0.003690888	36275	SS-CB(B)-700	0.285207612	15656
AG-CB(N)-500	0.058044983	36275	SS-CB(B)-300	0.285207612	15656
AG-CB(N)-700	0.063754325	36275	SS-CB(B)-500	0.285207612	15656
AG-CB(N)-900	0.088696655	36275	SS-CB(B)-900	0.2838812	15656
AG-CB(B)-100	0	36365	SS-CB(B)-100	0.269232987	15656
AG-CB(G)-100	0	36365	SS-CB(G)-100	0.224077278	15656
AG-CB(G)-300	0.015599769	36365	AG-CB(B)-500	0.16349481	36365
AG-CB(B)-300	0.024798155	36365	AG-CB(G)-500	0.13638985	36365
AG-CB(G)-900	0.083102653	36365	AG-CB(B)-700	0.133419839	36365
AG-CB(B)-900	0.100346021	36365	AG-CB(G)-700	0.113465975	36365
AG-CB(G)-700	0.113465975	36365	AG-CB(B)-900	0.100346021	36365
AG-CB(B)-700	0.133419839	36365	AG-CB(N)-700	0.088696655	36275
AG-CB(G)-500	0.13638985	36365	AG-CB(G)-900	0.083102653	36365
AG-CB(B)-500	0.16349481	36365	SS-CB(N)-100	0.075951557	15566
PB-CB(N)-100	0.06816609	37010	PB-CB(N)-100	0.06816609	37010
PB-CB(N)-300	0.855305652	37010	AG-CB(N)-500	0.063754325	36275
PB-CB(N)-500	0.873933103	37010	AG-CB(N)-900	0.058044983	36275
PB-CB(N)-700	0.89310842	37010	AG-CB(B)-300	0.024798155	36365
PB-CB(N)-900	0.898442907	37010	AG-CB(G)-300	0.015599769	36365
PB-CB(B)-100	0.682497116	37100	AG-CB(N)-300	0.003690888	36275
PB-CB(B)-300	0.864446367	37100	AG-CB(N)-100	0	36275
PB-CB(B)-500	0.882958478	37100	AG-CB(G)-100	0	36365
PB-CB(B)-700	0.911418685	37100	AG-CB(B)-100	0	36365
PB-CB(B)-900	0.931430219	37100	SQ-900	0	0
PB-CB(G)-100	0.950374856	37100	SQ-700	0	0
PB-CB(G)-300	0.950374856	37100	SQ-500	0	0
PB-CB(G)-500	0.950374856	37100	SQ-300	0	0
PB-CB(G)-700	0.950374856	37100	SQ-100	0	0

Table D1. Configuration, Effectiveness, and Annual Cost Sorted by Annual Cost and Effectiveness

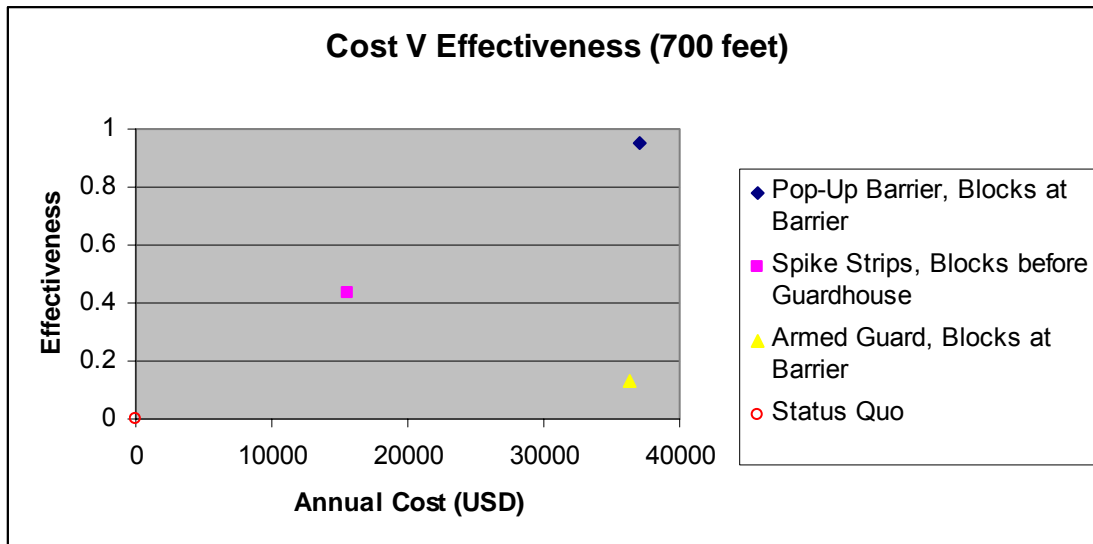


Figure D1. Cost vs Effectiveness of Alternatives at 700 Feet Range

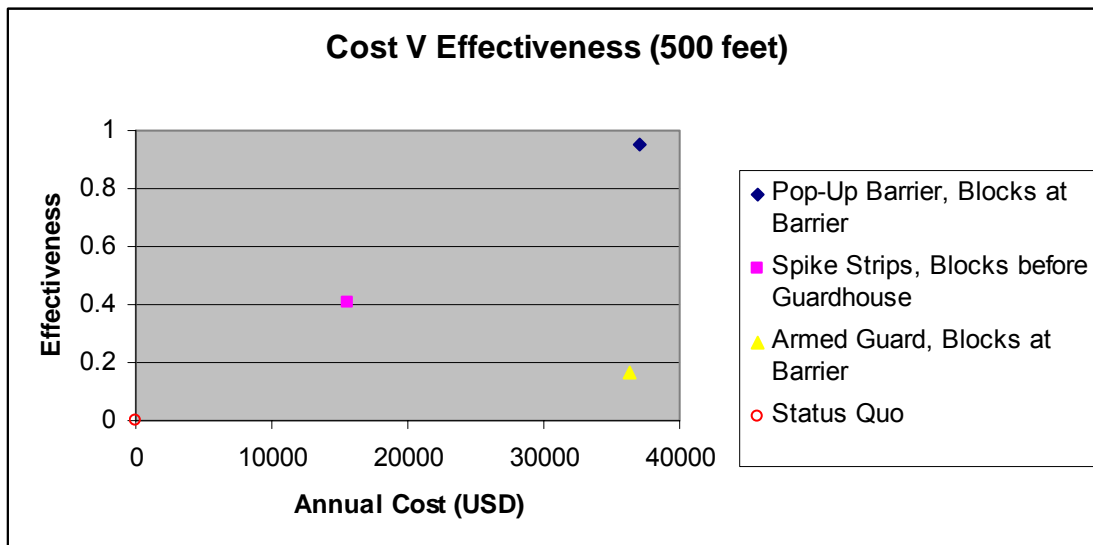


Figure D2. Cost vs Effectiveness of Alternatives at 500 Feet Range

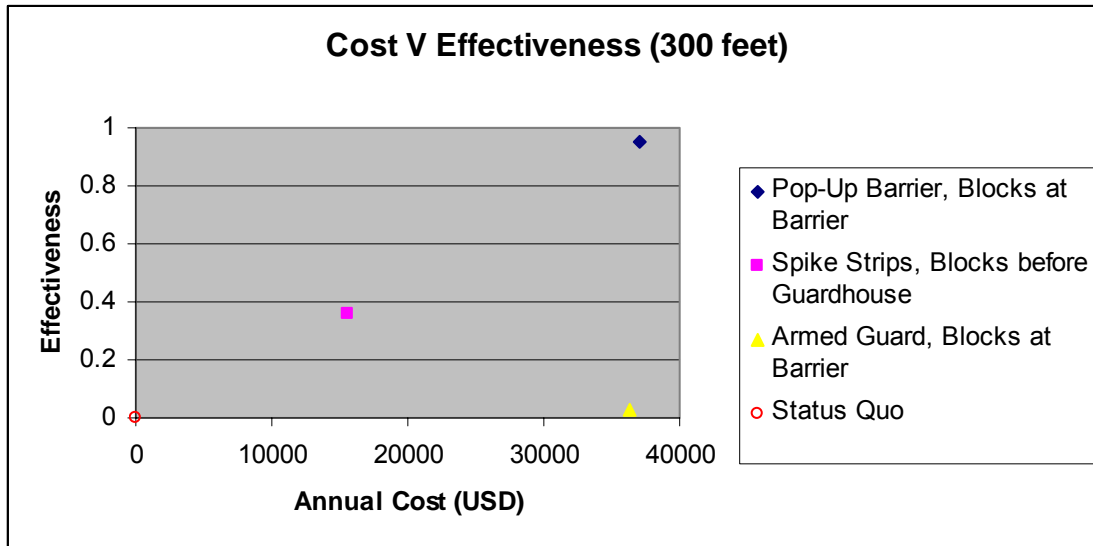


Figure D3. Cost vs Effectiveness of Alternatives at 300 Feet Range

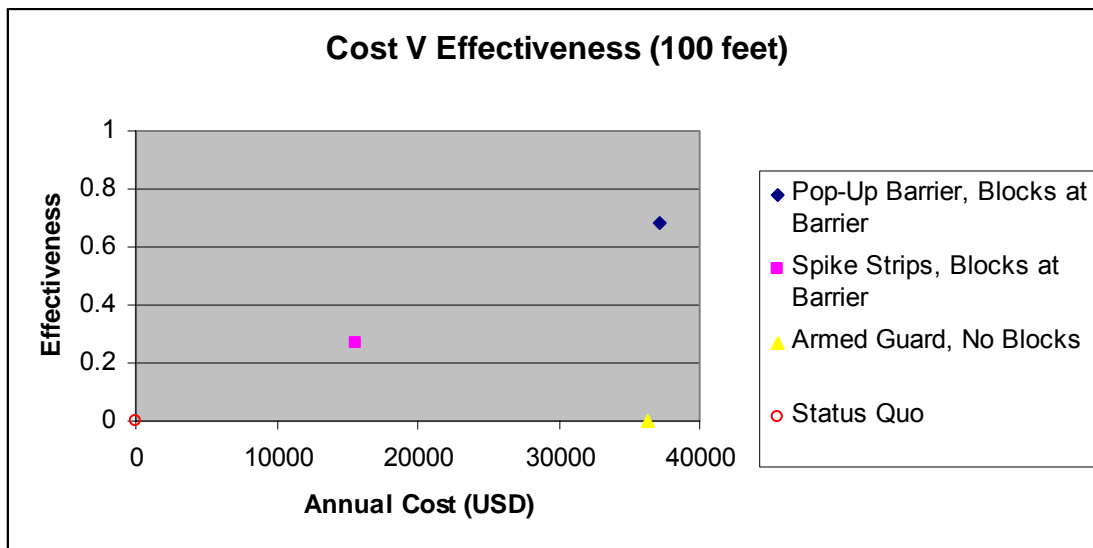


Figure D4. Cost vs Effectiveness of Alternatives at 100 Feet Range

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX E: SSTG MODELS

Design of Sensors

Each sensor was modeled for its probability of detection (P_{Detect}), false alarm rate and time to scan the object of interest.

The sensor's probability of detection was dependent on the type of materials being investigated. For instance, the chemical detector (used by the intrusive inspection team) is only effective at detecting chemical-contents of unwanted cargo and ineffective against any other types of material.

Gadget	Effectiveness Against Types of Material				False alarm	Time to Scan
	Radio-active	Bio-logical	Chemical	Explosives		
1 Scales					P_{FA}	T_{Scan}
2 Animals			P_{Detect}	P_{Detect}	P_{FA}	T_{Scan}
3 Radiation Detector (Passive)	P_{Detect}				P_{FA}	T_{Scan}
4 Gamma Scanner (Active)	P_{Detect}	P_{Detect}	P_{Detect}	P_{Detect}	P_{FA}	T_{Scan}
5 Biological detector		P_{Detect}			P_{FA}	T_{Scan}
6 Chemical detector			P_{Detect}		P_{FA}	T_{Scan}

Table E1: Performance of Sensors against Different Materials

Design of Sensor Suite

There are four areas where the sensors could be dispatched:

- At the point of entry into the source port (for incoming containers via land)
- Holding area where transshipment containers are stored
- On cranes where containers are loaded onto ships
- Intrusive inspection teams where containers are opened and searched.

The following table illustrates the possible configurations of sensors that are being modeled in this simulation. Over the multiple runs of the simulation, the following sensor configurations will be further varied by enabling or disabling these sensors at various inspection locations. The simulation of these different sensor configurations would allow for analysis of the difference in system performance due to each configuration.

	Sensor	Location of Sensor			
		Fixed Entry	Holding Area (Non Intrusive) Inspection	Intrusive Inspection	Crane (Non Intrusive) Inspection
1	Scales	X			X
2	Animals	X		X	
3	Radiation Detector (Passive)	X	X	X	X
4	Gamma Scanner (Active)	X	X	X	X
5	Biological detector			X	
6	Chemical detector			X	

Table E2: Use of Sensors at Various Inspection Locations

Summary of Sensor and Sensor Suite Design

Fixed Sensor Parameters		Levels
1	Probability of detection for each sensor, for each category of unwanted cargo	Location, sensor, material specific
2	Probability of false alarm for each sensor	Location, sensor specific
3	Time to scan container for each sensor	Location, sensor specific

Table E3: Fixed Sensor Parameters

Variable Sensor Suite Parameters		Levels
1	Availability of ATS	None, ATS, ATSpplus
2	Percentage of non-transshipment containers that goes through point of entry scanning	4 levels: 25%, 50%, 75%, 100%
3	Percentage of containers that is randomly selection for intrusive scanning	0-30%
4	Point of Entry – Availability of Scales	On/Off
5	Point of Entry – Availability of Trained Animals	On/Off
6	Point of Entry – Availability of Radiation Detectors	On/Off
7	Point of Entry – Availability of Gamma Scanners	On/Off
8	Holding Area Inspection – Availability of Radiation Detectors	On/Off
9	Holding Area Inspection – Availability of Gamma Scanners	On/Off
10	Intrusive Inspection – Availability of Trained Animals	On/Off
11	Intrusive Inspection – Availability of Radiation Detectors	On/Off
12	Intrusive Inspection – Availability of Gamma Scanners	On/Off
13	Intrusive Inspection – Availability of Biological Detectors	On/Off
14	Intrusive Inspection – Availability of Chemical Detectors	On/Off
15	Crane Inspection – Availability of Scales	On/Off
16	Crane Inspection – Availability of Radiation Detectors	On/Off
17	Crane Inspection – Availability of Gamma scanners	On/Off

Table E4: Variable Sensor Suite Parameters

Smart Design of Experiments using NOLH Algorithms

Both the Nearly-Orthogonal-Latin-Hypercube (NOLH) algorithm and its Extended NOLH version were considered for generating the sensor suite experiment points. The output experiment matrices from both algorithms were compared for correlation which should ideally be minimized to the ideal zero value. The ENOLH experiment matrix created an experiment matrix with higher average correlation but lesser critical correlation violations. Hence the ENOLH experiment is selected for use in this mode. The following two tables present the correlation between experiment factors using NOLH and ENOLH.

<i>NOLH</i>	<i>eScales</i>	<i>eAnimals</i>	<i>eRad</i>	<i>eGamma</i>	<i>hRad</i>	<i>hGamma</i>	<i>iAnimals</i>	<i>iRad</i>	<i>iGamma</i>	<i>iBio</i>	<i>iChem</i>	<i>cScales</i>	<i>cRad</i>	<i>cGamma</i>	<i>ATS</i>	<i>eScanPrc</i>	<i>iRdmSelPrc</i>
<i>eScales</i>	1.000																
<i>eAnimals</i>	0.008	1.000															
<i>eRad</i>	0.008	0.008	1.000														
<i>eGamma</i>	0.008	0.008	0.008	1.000													
<i>hRad</i>	0.008	0.008	0.008	0.008	1.000												
<i>hGamma</i>	0.070	0.008	0.008	0.008	0.008	1.000											
<i>iAnimals</i>	0.070	0.070	0.008	-0.054	0.008	-0.054	1.000										
<i>iRad</i>	0.039	-0.023	0.101	-0.085	0.101	-0.023	0.039	1.000									
<i>iGamma</i>	-0.023	-0.023	0.039	0.039	0.039	-0.023	-0.023	0.008	1.000								
<i>iBio</i>	0.008	0.008	-0.054	-0.054	0.008	0.008	0.008	-0.023	0.039	1.000							
<i>iChem</i>	-0.054	0.008	0.008	0.070	0.070	0.008	-0.054	-0.085	0.039	0.132	1.000						
<i>cScales</i>	0.101	0.039	0.039	-0.023	-0.023	-0.023	0.101	-0.054	-0.054	0.225	0.039	1.000					
<i>cRad</i>	-0.023	0.039	0.039	-0.023	-0.023	0.039	0.039	0.194	-0.054	0.039	-0.023	0.070	1.000				
<i>cGamma</i>	-0.054	0.008	0.008	0.008	0.070	-0.054	0.008	-0.023	0.039	-0.116	0.008	-0.023	-0.023	1.000			
<i>ATS</i>	-0.055	-0.077	0.120	-0.055	-0.098	-0.055	0.098	0.033	0.055	-0.033	-0.273	0.055	-0.011	-0.055	1.000		
<i>eScanPrc</i>	0.084	0.116	0.052	0.020	-0.076	-0.044	0.020	0.004	0.068	-0.044	0.020	0.004	0.004	-0.108	-0.006	1.000	
<i>iRdmSelPrc</i>	0.004	0.003	-0.054	0.010	-0.020	-0.008	-0.001	-0.054	0.006	-0.106	-0.013	-0.024	-0.022	-0.010	0.045	-0.054	1.000

Table E5: Correlation of Experimental Factors using NOLH

ENOLH65	eScales	eAnimals	eRad	eGamma	hRad	hGamma	iAnimals	iRad	iGamma	iBio	iChem	cScales	cRad	cGamma	ATS	eScanPrc	iRdmSelPrc
eScales	1																
eAnimals	0.015	1.000															
eRad	0.015	0.015	1.000														
eGamma	0.015	0.015	0.015	1.000													
hRad	0.015	0.015	0.015	0.015	1.000												
hGamma	0.015	0.015	0.015	0.015	0.015	1.000											
iAnimals	0.015	0.015	0.015	0.015	0.015	0.015	1.000										
iRad	-0.015	-0.015	-0.015	-0.015	-0.015	-0.015	-0.015	1.000									
iGamma	-0.015	-0.015	-0.015	-0.015	-0.015	-0.015	-0.015	0.015	1.000								
iBio	-0.015	-0.015	-0.015	-0.015	-0.015	-0.015	-0.015	0.015	0.015	1.000							
iChem	-0.015	-0.015	-0.015	-0.015	-0.015	-0.015	-0.015	0.015	0.015	0.015	1.000						
cScales	-0.015	-0.015	-0.015	-0.015	-0.015	-0.015	-0.015	0.015	0.015	0.015	0.015	1.000					
cRad	-0.015	-0.015	-0.015	-0.015	-0.015	-0.015	-0.015	0.015	0.015	0.015	0.015	0.015	1.000				
cGamma	-0.015	-0.015	-0.015	-0.015	-0.015	-0.015	-0.015	0.015	0.015	0.015	0.015	0.015	0.015	1.000			
ATS	0.094	-0.019	-0.057	-0.398	-0.095	0.094	-0.019	0.019	0.019	-0.019	0.057	0.057	-0.056	-0.208	1.000		
eScanPrc	0.180	-0.006	-0.006	-0.006	-0.169	0.180	-0.006	-0.017	0.006	-0.017	-0.017	0.006	-0.017	0.006	-0.050	1.000	
iRdmSelPrc	-0.008	0.002	-0.008	0.002	0.013	0.002	-0.105	0.051	0.019	0.051	-0.024	0.008	-0.024	0.019	0.003	0.007	1.000

Table E6: Correlation of Experimental Factors using ENOLH

	eScales	eAnimals	eRad	eGamma	hRad	hGamma	iAnimals	iRad	iGamma	iBio	iChem	cScales	cRad	cGamma	ATS	eScanPrc	iRdmSelPrc
1	1	0	0	0	0	0	1	1	1	1	1	1	1	1	2	1	0.05
2	1	1	0	0	0	0	0	0	0	0	1	1	1	1	2	1	0.06
3	1	0	1	0	0	0	0	1	1	1	0	0	0	1	2	1	0.07
4	1	1	1	0	0	0	1	0	0	0	0	0	0	1	2	1	0.04
5	1	0	0	1	0	0	1	0	1	1	0	1	1	0	0	1	0.06
6	1	1	0	1	0	0	0	1	0	0	0	1	1	0	0	1	0.05
7	1	0	1	1	0	0	0	0	1	1	1	0	0	0	0	1	0.05
8	1	1	1	1	0	0	1	1	0	0	1	0	0	0	0	1	0.06
9	1	0	0	0	1	0	1	1	0	1	1	0	1	0	2	0.25	0.03
10	1	1	0	0	1	0	0	0	1	0	1	0	1	0	2	0.25	0.08
11	1	0	1	0	1	0	0	1	0	1	0	1	0	0	2	0.25	0.08
12	1	1	1	0	1	0	1	0	1	0	0	1	0	0	2	0.25	0.03
13	1	0	0	1	1	0	1	0	0	1	0	0	1	1	0	0.25	0.07
14	1	1	0	1	1	0	0	1	1	0	0	0	1	1	0	0.25	0.04
15	1	0	1	1	1	0	0	0	0	1	1	1	0	1	0	0.25	0.04
16	1	1	1	1	1	0	1	1	1	0	1	1	0	1	0	0.25	0.07
17	1	0	0	0	0	1	1	1	1	0	1	1	0	1	1	0.5	0.02
18	1	1	0	0	0	1	0	0	0	1	1	1	0	1	1	0.5	0.09
19	1	0	1	0	0	1	0	1	1	0	0	0	1	1	1	0.5	0.09
20	1	1	1	0	0	1	1	0	0	1	0	0	1	1	0	0.5	0.02
21	1	0	0	1	0	1	1	0	1	0	0	1	0	0	2	0.5	0.08
22	1	1	0	1	0	1	0	1	0	1	0	1	0	0	2	0.5	0.03
23	1	0	1	1	0	1	0	0	1	0	1	0	1	0	2	0.5	0.02
24	1	1	1	1	0	1	1	1	0	1	1	0	1	0	2	0.5	0.08
25	1	0	0	0	1	1	1	1	0	0	1	0	0	0	1	1	0.01
26	1	1	0	0	1	1	0	0	1	1	1	0	0	0	1	1	0.10

	eScales	eAnimals	eRad	eGamma	hRad	hGamma	iAnimals	iRad	iGamma	iBio	iChem	cScales	cRad	cGamma	ATS	eScanPrc	iRdmSelPrc
27	1	0	1	0	1	1	0	1	0	0	0	1	1	0	1	1	0.10
28	1	1	1	0	1	1	1	0	1	1	0	1	1	0	1	1	0.01
29	1	0	0	1	1	1	1	0	0	0	0	0	0	1	1	1	0.10
30	1	1	0	1	1	1	0	1	1	1	0	0	0	1	1	1	0.02
31	1	0	1	1	1	1	0	0	0	0	1	1	1	1	1	1	0.01
32	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0.10
33	1	1	1	1	1	1	1	0	0	0	0	0	0	0	1	0.75	0.06
34	0	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0.25	0.06
35	0	0	1	1	1	1	1	1	1	1	0	0	0	0	0	0.25	0.05
36	0	1	0	1	1	1	1	0	0	0	1	1	1	0	0	0.25	0.04
37	0	0	0	1	1	1	0	1	1	1	1	1	1	0	0	0.25	0.07
38	0	1	1	0	1	1	0	1	0	0	1	0	0	1	2	0.25	0.05
39	0	0	1	0	1	1	1	0	1	1	1	0	0	1	2	0.25	0.06
40	0	1	0	0	1	1	1	1	0	0	0	1	1	1	2	0.25	0.06
41	0	0	0	0	1	1	0	0	1	1	0	1	1	1	2	0.25	0.05
42	0	1	1	1	0	1	0	0	1	0	0	1	0	1	0	1	0.08
43	0	0	1	1	0	1	1	1	0	1	0	1	0	1	0	1	0.04
44	0	1	0	1	0	1	1	0	1	0	1	0	1	1	0	1	0.03
45	0	0	0	1	0	1	0	1	0	1	1	0	1	1	0	1	0.08
46	0	1	1	0	0	1	0	1	1	0	1	1	0	0	2	1	0.04
47	0	0	1	0	0	1	1	0	0	1	1	1	0	0	2	1	0.07
48	0	1	0	0	0	1	1	1	1	0	0	0	1	0	2	1	0.07
49	0	0	0	0	0	1	0	0	0	1	0	0	1	0	2	1	0.04
50	0	1	1	1	1	0	0	0	0	1	0	0	1	0	1	0.75	0.09
51	0	0	1	1	1	0	1	1	1	0	0	0	1	0	1	0.75	0.02
52	0	1	0	1	1	0	1	0	0	1	1	1	0	0	2	0.75	0.02
53	0	0	0	1	1	0	0	1	1	0	1	1	0	0	2	0.75	0.09
54	0	1	1	0	1	0	0	1	0	1	1	0	1	1	0	0.75	0.03
55	0	0	1	0	1	0	1	0	1	0	1	0	1	1	0	0.75	0.08
56	0	1	0	0	1	0	1	1	0	1	0	1	0	1	0	0.75	0.09
57	0	0	0	0	1	0	0	0	1	0	0	1	0	1	0	1	0.03
58	0	1	1	1	0	0	0	0	1	1	0	1	1	1	1	0.25	0.10
59	0	0	1	1	0	0	1	1	0	0	0	1	1	1	1	0.25	0.01
60	0	1	0	1	0	0	1	0	1	1	1	0	0	1	1	0.25	0.01
61	0	0	0	1	0	0	0	1	0	0	1	0	0	1	1	0.25	0.10
62	0	1	1	0	0	0	0	1	1	1	1	1	1	0	1	0.25	0.02
63	0	0	1	0	0	0	1	0	0	0	1	1	1	0	1	0.25	0.09
64	0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	0.25	0.10
65	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0.25	0.01

Table E7: Values for Experimental Design of Sensor Suites using ENOLH

APPENDIX F: SSTG METRICS

The following list the Measures of Effectiveness (MOE), Measures of Performance (MOP) to be evaluated and the Data Requirement (DR) to be collected from the simulations.

1. MOE: Accuracy of Inspections

For each inspection location, the following MOPs are evaluated.

1) MOP: Probability of detecting undesired cargo

- 1.1.1. DR: Number of clean containers that arrived at inspection location
- 1.1.2. DR: Number of dirty containers that arrived at inspection location
- 1.1.3. DR: Number of clean containers that started inspection
- 1.1.4. DR: Number of dirty containers that started inspection
- 1.1.5. DR: Number of clean containers that completed inspection and passed
- 1.1.6. DR: Number of dirty containers that completed inspection and failed

2) MOP: Probability of False Alarm

- 1.2.1. DR: Number of clean containers that arrived at inspection location
- 1.2.2. DR: Number of clean containers that started inspection
- 1.2.3. DR: Number of clean containers that completed inspection and failed

3) MOP: Probability of Miss Detection

- 1.3.1. DR: Number of dirty containers that arrived at inspection location
- 1.3.2. DR: Number of dirty containers that started inspection
- 1.3.3. DR: Number of dirty containers that completed inspection and passed

2. MOE: Timeliness of Inspections

For each inspection location, the following MOPs are evaluated.

1) MOP: Average Handling time per container

- 2.1.1. DR: Total time duration
- 2.1.2. DR: Average queue length of inspection server
- 2.1.3. DR: Number of containers in queue
- 2.1.4. DR: Average time in queue
- 2.1.5. DR: Time arrive at inspection station
- 2.1.6. DR: Time leave inspection station

2.1.7. DR: Average time in inspection server

2.1.8. DR: Time start inspection

2.1.9. DR: Time end inspection

2) MOP: Container throughput

2.3.1. DR: Total time duration

2.3.2. DR: Number of containers arriving at inspection location

2.3.3. DR: Number of containers that received service

Simulation Output Parameter	Parameter Name	Type
<u>General</u>		
Run Index	RunIdx	Integer [1-33]
Iteration Index	IterationIdx	Integer [1-10]
Time Start Simulation	tStartSim	Integer [Seconds]
Time End Simulation	tStopSim	Integer [Seconds]
Number of dirty containers detained	numDirtyDetained	Integer [Containers]
Number of clean containers detained	numCleanDetained	Integer [Containers]

Table F1: Simulation ‘General’ Output Parameters

Simulation Output Parameter	Parameter Name	Type
<u>Per server at inspection location</u>		
Percentage of time that inspection server is idle	cPrctIdle	Double [0-1]
Percentage of time that inspection server is busy	cPrctUtilization	Double [0-1]

Table F2: Simulation ‘Per Server at Inspection Location’ Output Parameters

Simulation Output Parameter	Parameter Name	Type
<u>Per ship index N</u>		
Time start load ship	tStartLoadShip	Integer [Seconds]
Time stop load ship	tStopLoadShip	Integer [Seconds]
Number of dirty containers loaded on board	numDirtyLoadedOnShip	Integer [Containers]

Table F3: Simulation ‘Per Ship Index N’ Output Parameters

Simulation Output Parameter	Parameter Name	Type
<u>Per inspection location</u>		
Number of containers that arrived at inspection location	cNumContainersArrive	Integer [Containers]
Number of clean containers that arrived at inspection location	cNumCleanContainersArrive	Integer [Containers]
Number of dirty containers that arrived at inspection location	cNumDirtyContainersArrive	Integer [Containers]
Number of containers that started service	cNumContainersStart	Integer [Containers]
Number of clean containers that started inspection	cNumCleanContainersStart	Integer [Containers]
Number of dirty containers that started inspection	cNumDirtyContainersStart	Integer [Containers]
Number of containers that completed service	cNumContainersComplete	Integer [Containers]
Number of clean containers that completed inspection and passed	cNumCleanPass	Integer [Containers]
Number of clean containers that completed inspection and failed	cNumCleanFail	Integer [Containers]
Number of dirty containers that completed inspection and passed	cNumDirtyPass	Integer [Containers]
Number of dirty containers that completed inspection and failed	cNumDirtyFail	Integer [Containers]
Average queue length of inspection server	cAvgLengthOfQueue	Integer [Containers]
Average time in inspection server	cAvgTimeInServer	Integer [Seconds]
Average time in queue	cAvgTimeInQueue	Integer [Seconds]

Table F4: Simulation ‘Per Inspection Location’ Output Parameters

APPENDIX G: SSTG INPUT PARAMETERS

Fixed Simulation Parameters

The table and the following page lists the input simulation parameters that will be fixed for all simulation runs. The fixed simulation parameters can be broadly categorized into the following groups:

- General
- Container Generation
- Ship Scheduling
- ATS
- Fixed point of entry
- Holding area (non-intrusive) inspection
- Crane (non-intrusive) Inspection
- Intrusive Inspection
- Sensor Parameters

	Fixed Simulation Parameter	Parameter Name	Type	Default Value
1	<u>General</u>			
	Time to start simulation	tStartSim	Integer [Seconds]	0
	Time to stop simulation	tStopSim	Integer [Seconds]	43200
2	<u>Ship Scheduling</u>			
	Time ship 1 sails	tShip1Sail	Integer [Seconds]	
	Time ship 2 sails	tShip2Sail	Integer [Seconds]	
	Time ship 3 sails	tShip3Sail	Integer [Seconds]	
	Number of containers to be loaded to ship 1	numContainersToLoadOnShip1	Integer [Containers]	
	Number of containers to be loaded to ship 2	numContainersToLoadOnShip2	Integer [Containers]	
	Number of containers to be loaded to ship 3	numContainersToLoadOnShip3	Integer [Containers]	
3	<u>Container Generation</u>			
	Number of containers in storage at beginning of run	numInitHoldingAreaContainers	Integer [Containers]	
	Number of transshipment containers to create	numCreateTransContainers	Integer [Containers]	
	Number of containers incoming via truck to create	numCreateTruckContainers	Integer [Containers]	
	Number of containers incoming via rail to create	numCreateRailContainers	Integer [Containers]	
4	<u>ATS</u>			
	Percentage of manifests with discrepancies	prcManifestDiscrepancy	Double [0-1]	0.05
	Percentage of containers that are marked hi-risk by ATS	atsHiRiskPrc	Double [0-1]	0.06
5	<u>Fixed Point of Entry</u>			
	Number of servers (lanes) at the point of entry	eNumServersPerGate	Integer [Servers per gate]	2
6	<u>Holding Area</u>			
	Number of servers (mobile non-intrusive scanners) at the holding areas	hNumServers	Integer [Servers]	5
7	<u>Cranes / Ship Loading Area</u>			
	Number of servers (cranes) per ship at the loading bay	cNumServersPerShip	Integer [Servers per ship]	6
	Time crane takes to load a clean container	tCraneHandleCleanContainer	Integer [Seconds]	60
	Time crane takes to handle a suspect container	tCraneHandleSuspectContainer	Integer [Seconds]	120
8	<u>Intrusive Inspection</u>			
	Number of servers (inspection teams) for intrusive inspection	iNumServers	Integer [Servers]	10

Table G1: Fixed Simulation Parameters in Extend Data Array

Fixed Sensor Simulation Parameter At Point of Entry	Parameter Name	Type	Global Array in Extend	Col	Row	Default Value
Probability of false alarms by scales at point of entry	sScalesPfa	Double [0-1]	gFEntry	1	2	0.1
Time of scan by scales at point of entry	sScalesTscan	Double [Seconds]	gFEntry	1	7	10
Probability of false alarms by trained animals at point of entry	aAnimalsPfa	Double [0-1]	gFEntry	2	2	0.1
Probability of detection of chemical-content cargo by trained animals at point of entry	aAnimalsPdChem	Double [0-1]	gFEntry	2	3	0.9
Probability of detection of explosives-content cargo by trained animals at point of entry	aAnimalsPdExp1	Double [0-1]	gFEntry	2	4	0.9
Time of scan by trained animals at point of entry	aAnimalsTscan	Double [Seconds]	gFEntry	2	7	10
Probability of false alarms by radiation detectors at point of entry	rRadPfa	Double [0-1]	gFEntry	3	2	0.1
Probability of detection of radioactive-content cargo by radiation detectors at point of entry	rRadPdRad	Double [0-1]	gFEntry	3	3	0.9
Time of scan by radiation detectors at point of entry	rRadTscan	Double [Seconds]	gFEntry	3	7	10
Probability of false alarms by gamma scanners at point of entry	gGammaPfa	Double [0-1]	gFEntry	4	2	0.1
Probability of detection of radioactive-content cargo by gamma scanners at point of entry	gGammaPdRad	Double [0-1]	gFEntry	4	3	0.9
Probability of detection of biological-content cargo by gamma scanners at point of entry	gGammaPdBio	Double [0-1]	gFEntry	4	4	0.9
Probability of detection of chemical-content cargo by gamma scanners at point of entry	gGammaPdChem	Double [0-1]	gFEntry	4	5	0.9
Probability of detection of explosives-content cargo by gamma scanners at point of entry	gGammaPdExp1	Double [0-1]	gFEntry	4	6	0.9
Time of scan by gamma scanners at point of entry	gGammaTscan	Double [Seconds]	gFEntry	4	7	10

Table G2: Fixed Sensor Simulation Parameters for Location: Point of Entry

Fixed Sensor Simulation Parameter At Holding Area	Parameter Name	Type	Global Array in Extend	Col	Row	Default Value
Probability of false alarms by radiation detectors at holding area inspections	hRadPfa	Double [0-1]	gFHolding	1	2	0.2
Probability of detection of radioactive-content cargo by radiation detectors at holding area inspections	hRadPdRad	Double [0-1]	gFHolding	3	3	0.9
Time of scan by radiation detectors at holding area inspections	hRadTscan	Double [Seconds]	gFHolding	3	7	10
Probability of false alarms by gamma scanners at holding area inspections	hGammaPfa	Double [0-1]	gFHolding	4	2	0.1
Probability of detection of radioactive-content cargo by gamma scanners at holding area inspections	hGammaPdRad	Double [0-1]	gFHolding	4	3	0.9
Probability of detection of biological-content cargo by gamma scanners at holding area inspections	hGammaPdBio	Double [0-1]	gFHolding	4	4	0.9
Probability of detection of chemical-content cargo by gamma scanners at holding area inspections	hGammaPdChem	Double [0-1]	gFHolding	4	5	0.9
Probability of detection of explosives-content cargo by gamma scanners at holding area inspections	hGammaPdExp1	Double [0-1]	gFHolding	4	6	0.9
Time of scan by gamma scanners at holding area inspections	hGammaTscan	Double [Seconds]	gFHolding	4	7	10

Table G3: Fixed Sensor Simulation Parameters for Location: Holding Area (Non-Intrusive Inspection)

Fixed Sensor Simulation Parameter At Intrusive Inspection Teams	Parameter Name	Type	Global Array in Extend	Col	Row	Default Value
Probability of false alarms by trained animals in intrusive inspection teams	iAnimalsPfa	Double [0-1]	gIntrusive	2	2	0.1
Probability of detection of chemical-content cargo by trained animals in intrusive inspection teams	iAnimalsPdChem	Double [0-1]	gIntrusive	2	5	0.9
Probability of detection of explosive-content cargo by trained animals in intrusive inspection teams	iAnimalsPdExp1	Double [0-1]	gIntrusive	2	6	0.9
Time of scan by trained animals at intrusive inspection teams	iAnimalsTscan	Double [Seconds]	gIntrusive	2	7	10
Probability of false alarms by radiation detectors in intrusive inspection teams	iRadPfa	Double [0-1]	gIntrusive	3	2	0.2
Probability of detection of radioactive-content cargo by radiation detectors in intrusive inspection teams	iRadPdRad	Double [0-1]	gIntrusive	3	3	0.9
Time of scan by radiation detectors at intrusive inspection teams	iRadTscan	Double [Seconds]	gIntrusive	3	7	10
Probability of false alarms by gamma scanners in intrusive inspection teams	iGammaPfa	Double [0-1]	gIntrusive	4	2	0.1
Probability of detection of radioactive-content cargo by gamma scanners in intrusive inspection teams	iGammaPdRad	Double [0-1]	gIntrusive	4	3	0.9
Probability of detection of biological content cargo by gamma scanners in intrusive inspection teams	iGammaPdBio	Double [0-1]	gIntrusive	4	4	0.9
Probability of detection of chemical-content cargo by gamma scanners in intrusive inspection teams	iGammaPdChem	Double [0-1]	gIntrusive	4	5	0.9
Probability of detection of explosive-content cargo by gamma scanners in intrusive inspection teams	iGammaPdExp1	Double [0-1]	gIntrusive	4	6	0.9
Time of scan by gamma scanners at intrusive inspection teams	iGammaTscan	Double [Seconds]	gIntrusive	4	7	10
Probability of false alarms by biological detectors in intrusive inspection teams	iBioPfa	Double [0-1]	gIntrusive	5	2	0.1
Probability of detection of biological-content cargo by biological detectors in intrusive inspection teams	iBioPdBio	Double [0-1]	gIntrusive	5	4	0.9
Time of scan by biological detectors at intrusive inspection teams	iBioTscan	Double [Seconds]	gIntrusive	5	7	10
Probability of false alarms by chemical detectors in intrusive inspection teams	iChemPfa	Double [0-1]	gIntrusive	5	2	0.1
Probability of detection of chemical-content cargo by chemical detectors in intrusive inspection teams	iChemPdChem	Double [0-1]	gIntrusive	5	5	0.9
Time of scan by chemical detectors at intrusive inspection teams	iChemTscan	Double [Seconds]	gIntrusive	5	7	10

Table G4: Fixed Sensor Simulation Parameters for Location: Intrusive Inspection Teams

Fixed Sensor Simulation Parameter At Cranes	Parameter Name	Type	Global Array in Extend	Col	Row	Default Value
Probability of false alarms by scales on cranes	cScaledPfa	Double [0-1]	gCranee	1	2	0.1
Time of scan by scales at cranes	cScaledTscan	Double [Seconds]	gCranee	1	7	10
Probability of false alarms by radiation detectors on cranes	cRadPfa	Double [0-1]	gCranee	3	2	0.1
Probability of detection of radioactive-content cargo by radiation detectors on cranes	cRadPdRad	Double [0-1]	gCranee	3	3	0.9
Time of scan by radiation detectors at cranes	cRadTscan	Double [Seconds]	gCranee	3	7	10
Probability of false alarms by gamma scanners on cranes	cGammaPfa	Double [0-1]	gCranee	4	2	0.1
Probability of detection of radioactive-content cargo by gamma scanners on cranes	cGammaPdRad	Double [0-1]	gCranee	4	3	0.9
Time of scan by gamma scanners at cranes	cGammaTscan	Double [Seconds]	gCranee	4	7	10

Table G5: Fixed Sensor Simulation Parameters for Location: Cranes

The following table shows the organization of parameters for the combination of sensors at each of the locations: fixed entry point, non-intrusive inspection, intrusive inspection and cranes. In Extend, there will be a global data array created for each location. Within each data array, the parameter is accessed via its specific column and row index.

	Scales	Animals	Radiation Detector (Passive)	Gamma Scanner (Active)	Biological detector	Chemical detector
Possibility of sensor on platform	(1,1) Row1, Col1	(1,2)	(1,3)	(1,4)	(1,5)	(1,6)
P_{FA}	(2,1)	(2,2)	(2,3)	(2,4)	(2,5)	(2,6)
P_{Detect} against radioactive material	(3,1)	(3,2)	(3,3)	(3,4)	(3,5)	(3,6)
P_{Detect} against biological material	(4,1)	(4,2)	(4,3)	(4,4)	(4,5)	(4,6)
P_{Detect} against chemical material	(5,1)	(5,2)	(5,3)	(5,4)	(5,5)	(5,6)
P_{Detect} against explosive material	(6,1)	(6,2)	(6,3)	(6,4)	(6,5)	(6,6)
Tscan	(7,1)	(7,2)	(7,3)	(7,4)	(7,5)	(7,6)

Table G6: Organization of Sensor Parameters in Data Array for Each Location

Variable Simulation Parameters

The following table lists the 17 input simulation parameters that will be varied for all simulation runs. For each simulation, there will be different combinations of sensors selected, as well as different percentages of selection for various purposes.

	Variable Simulation Parameter	Parameter Name	Type	Global Array in Extend
	POINT OF ENTRY			
1	Availability of scales at point of entry	eScales	Boolean	gvExpt
2	Availability of trained animals at point of entry	eAnimals	Boolean	gvExpt
3	Availability of radiation detectors at point of entry	eRad	Boolean	gvExpt
4	Availability of gamma scanners at point of entry	eGamma	Boolean	gvExpt
	HOLDING AREA (NON-INTRUSIVE) INSPECTION TEAMS			
5	Availability of radiation detectors at holding area inspections	hRad	Boolean	gvExpt
6	Availability of gamma scanners at holding area inspections	hGamma	Boolean	gvExpt
	INTRUSIVE INSPECTION TEAMS			
7	Availability of trained animals in intrusive inspection teams	iAnimals	Boolean	gvExpt
8	Availability of radiation detectors in intrusive inspection teams	iRad	Boolean	gvExpt
9	Availability of gamma scanners in intrusive inspection teams	iGamma	Boolean	gvExpt
10	Availability of biological detectors in intrusive inspection teams	iBio	Boolean	gvExpt
11	Availability of chemical detectors in intrusive inspection teams	iChem	Boolean	gvExpt
	CRANES INSPECTION			
12	Availability of scales on cranes	cScales	Boolean	gvExpt
13	Availability of radiation detectors on cranes	cRad	Boolean	gvExpt
14	Availability of gamma scanners on cranes	cGamma	Boolean	gvExpt
	GENERAL			
15	Availability of ATS	ATS	Integer 0: None 1: AIS 2: ATS+	gvExpt
16	Percentage of containers that is randomly selected for intrusive scanning	iRdmSePrc	Double 4 levels: 25%, 50%, 75%, 100%	gvExpt
17	Percentage of non-shipment containers that goes through point of entry scanning	eScanPrc	Double	gvExpt

Table G7: Variable Simulation Parameters

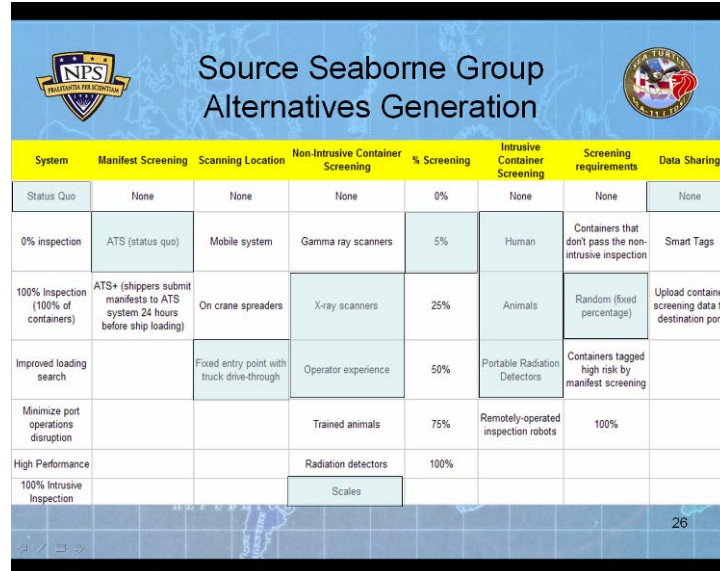
APPENDIX H: SSTG ALTERNATIVE PARAMETER SETTINGS

The container screening model is configured to simulate the performance of the status quo system and its alternatives formulated during alternative generation. This appendix describes the model configuration of the status quo systems and its six alternatives.

- Status Quo
- “100% (Volume) Non-Intrusive Inspection” Alternative
- “Improved Loading Search” Alternative
- “Minimize Port Operations” Alternative
- “High Performance” Alternative
- “100% (Volume) Intrusive Inspection” Alternative

There is a limitation in how precise the model configuration can represent each of the alternatives exactly as described earlier. The container screening model was designed to be sufficiently general in order to answer the bigger issue of optimal sensor mix. Hence it does not model precise container handling procedures that could be unique to one single alternative. Nonetheless, concessions are made to represent the alternatives in the model as close as possible.

Status Quo



System	Manifest Screening	Scanning Location	Non-Intrusive Container Screening	% Screening	Intrusive Container Screening	Screening requirements	Data Sharing
Status Quo	None	None	None	0%	None	None	None
0% inspection	ATS (status quo)	Mobile system	Gamma ray scanners	5%	Human	Containers that don't pass the non-intrusive inspection	Smart Tags
100% Inspection (100% of containers)	ATS+ (shippers submit manifests to ATS system 24 hours before ship loading)	On crane spreaders	X-ray scanners	25%	Animals	Random (fixed percentage)	Upload container screening data to destination port
Improved loading search		Fixed entry point with truck drive-through	Operator experience	50%	Portable Radiation Detectors	Containers tagged high risk by manifest screening	
Minimize port operations disruption			Trained animals	75%	Remotely-operated inspection robots	100%	
High Performance			Radiation detectors	100%			
100% Intrusive Inspection			Scales				

Alternative	eScales	eAnimals	eRad	eGamma	
Status Quo	Yes	No	No	Yes	
	hRad	hGamma			
	No	No			
	iAnimals	iRad	iGamma	iBio	iChem
	Yes	Yes	No	No	No
	cScales	cRad	cGamma		
	No	No	No		
	ATS	eScanPrc	iRdmSelPrc		
	ATS - StatusQuo	5%	6%		

Figure H1. Experiment Configuration of Status Quo

The first system to be modeled is the status quo system, which represents the current state of affairs. The performance of the alternative systems will be benchmarked with the status quo system, wherever appropriate.

The status quo system has the default ATS system, scales and Gamma scanners at fixed point of entry (equivalent to X-ray scanners, which are not modeled in the simulation), and scans 5% (eScanPrc factor) of incoming land containers at its fixed point of entry. A random percentage of containers (iRdmSelPrc = 6%) is selected for examination by the intrusive inspection team, which is equipped with trained animals and radiation detectors. The status quo system does not have any mobile non-intrusive

scanning teams nor does it equip its cranes with scanners, which means that transshipment cargo is not inspected at all.

“100% (Volume) Non-Intrusive Inspection” Alternative

Source Seaborne Group Alternatives Generation							
System	Manifest Screening	Scanning Location	Non-Intrusive Container Screening	% Screening	Intrusive Container Screening	Screening requirements	Data Sharing
Status Quo	None	None	None	0%	None	None	None
0% inspection	ATS (status quo)	Mobile system	Gamma ray scanners	5%	Human	Containers that don't pass the non-intrusive inspection	Smart Tags
100% inspection (100% of containers)	ATS+ (shippers submit manifests to ATS system 24 hours before ship loading)	On crane spreaders	X-ray scanners	25%	Animals	Random (fixed percentage)	Upload container screening data to destination port
Improved loading search		Fixed entry point with truck drive-through	Operator experience	50%	Portable Radiation Detectors	Containers tagged high risk by manifest screening	
Minimize port operations disruption			Trained animals	75%	Remotely-operated inspection robots	100%	
High Performance			Radiation detectors	100%			
100% Intrusive Inspection			Scales				

Alternative	eScales	eAnimals	eRad	eGamma	
1	Yes	No	Yes	Yes	
	hRad	hGamma			
	No	No			
	iAnimals	iRad	iGamma	iBio	iChem
	Yes	Yes	No	No	No
	cScales	cRad	cGamma		
	Yes	Yes	Yes		
	ATS	eScanPrc	iRdmSelPrc		
	None	100%	0%		

Figure H2: Experiment Configuration of Alternative 1

The “100% (Volume) Non-Intrusive Inspection” alternative scans 100% of incoming land containers (eScanPrc = 1) at the fixed point of entry and 100% of all containers while loading on the cranes. Both the fixed point entry and cranes are equipped with scales radiation detectors and Gamma scanners (equivalent to X-ray scanners, which are not modeled in the simulation). The intrusive inspection team, equipped with trained animals and radiation detectors, only processes previously failed

containers and nothing is randomly selected for inspection. Given that 100% of all containers will be non-intrusively searched, there is no need for ATS profiling.

“Improved Loading Search” Alternative

Source Seaborne Group Alternatives Generation							
System	Manifest Screening	Scanning Location	Non-Intrusive Container Screening	% Screening	Intrusive Container Screening	Screening requirements	Data Sharing
Status Quo	None	None	None	0%	None	None	None
0% inspection	ATS (status quo)	Mobile system	Gamma ray scanners	5%	Human	Containers that don't pass the non-intrusive inspection	Smart Tags
100% Inspection (100% of containers)	ATS+ (shippers submit manifests to ATS system 24 hours before ship loading)	On crane spreaders	X-ray scanners	25%	Animals	Random (fixed percentage)	Upload container screening data to destination port
Improved loading search		Fixed entry point with truck drive-through	Operator experience	50%	Portable Radiation Detectors	Containers tagged high risk by manifest screening	
Minimize port operations disruption			Trained animals	75%	Remotely-operated inspection robots	100%	
High Performance			Radiation detectors	100%			
100% Intrusive Inspection			Scales				

Alternative	eScales	eAnimals	eRad	eGamma	
2	No	No	No	No	
	hRad	hGamma			
	No	No			
	iAnimals	iRad	iGamma	iBio	iChem
	Yes	Yes	No	No	No
	cScales	cRad	cGamma		
	Yes	Yes	Yes		
	ATS	eScanPrc	iRdmSelPrc		
	ATS - StatusQuo	0%	0%		

Figure H3. Experiment Configuration of Alternative 2

The “Improved Loading Search” alternative is an incremental solution on top of the status quo system in place. This alternative emphasizes sensors on the crane for loading containers for shipment, i.e. scales, radiation detectors, while skipping the rest of the sensors. It includes the current ATS risk profiling to select high risk containers for intrusive inspection, which is added by an adequate sensor suite of trained animals and radiation detectors.

“Minimize Disruption to Port Operations” Alternative

Source Seaborne Group Alternatives Generation							
System	Manifest Screening	Scanning Location	Non-Intrusive Container Screening	% Screening	Intrusive Container Screening	Screening requirements	Data Sharing
Status Quo	None	None	None	0%	None	None	None
0% inspection	ATS (status quo)	Mobile system	Gamma ray scanners	5%	Human	Containers that don't pass the non-intrusive inspection	Smart Tags
100% inspection (100% of containers)	ATS+ (shippers submit manifests to ATS system 24 hours before ship loading)	On crane spreaders	X-ray scanners	25%	Animals	Random (fixed percentage)	Upload container screening data to destination port
Improved loading search		Fixed entry point with truck drive-through	Operator experience	50%	Portable Radiation Detectors	Containers tagged high risk by manifest screening	
Minimize port operations disruption			Trained animals	75%	Remotely-operated inspection robots	100%	
High Performance			Radiation detectors	100%			
100% Intrusive Inspection			Scales				

Alternative	eScales	eAnimals	eRad	eGamma	
3	No	No	No	No	
	hRad	hGamma			
	No	No			
	iAnimals	iRad	iGamma	iBio	iChem
	No	No	No	No	No
	cScales	cRad	cGamma		
	Yes	Yes	Yes		
	ATS	eScanPrc	iRdmSelPrc		
	ATS - Plus	0%	0%		

Figure H4. Experiment Configuration of Alternative 3

The “Minimize Disruption to Port Operations” Alternative seeks to improve probability of detection and deterrence with better pre-emption of high-risk containers, as well as smooth-integration of its inspection processes within port operations. Thus this alternative includes the ATS-plus system that targets dirty containers better and emphasizes crane sensors, i.e. scales, radiation detectors, while skipping the rest of the sensors.

“High Performance” Alternative

Source Seaborne Group Alternatives Generation							
System	Manifest Screening	Scanning Location	Non-Intrusive Container Screening	% Screening	Intrusive Container Screening	Screening requirements	Data Sharing
Status Quo	None	None	None	0%	None	None	None
0% inspection	ATS (status quo)	Mobile system	Gamma ray scanners	5%	Human	Containers that don't pass the non-intrusive inspection	Smart Tags
100% Inspection (100% of containers)	ATS+ (shippers submit manifests to ATS system 24 hours before ship loading)	On crane spreaders	X-ray scanners	25%	Animals	Random (fixed percentage)	Upload container screening data to destination port
Improved loading search		Fixed entry point with truck drive-through	Operator experience	50%	Portable Radiation Detectors	Containers tagged high risk by manifest screening	
Minimize port operations disruption			Trained animals	75%	Remotely-operated inspection robots	100%	
High Performance			Radiation detectors	100%			
100% Intrusive Inspection			Scales				

Alternative	eScales	eAnimals	eRad	eGamma	
4	No	No	No	No	
	hRad	hGamma			
	Yes	Yes			
	iAnimals	iRad	iGamma	iBio	iChem
	Yes	Yes	Yes	No	No
	cScales	cRad	cGamma		
	Yes	Yes	Yes		
	ATS	eScanPrc	iRdmSelPrc		
	ATS - Plus	0%	0%		

Figure H5. Experiment Configuration of Alternative 4

The “High Performance” Alternative seeks to improve probability of detection and deterrence with better pre-emption of high-risk containers and layered inspections. This alternative focuses on transshipment containers, which form the bulk of container traffic in this port simulation. Thus sensors are deployed in the holding area and during crane loading. It also includes the ATS-plus system that targets dirty containers better.

“100% (Volume) Intrusive Inspection” Alternative

Source Seaborne Group Alternatives Generation							
System	Manifest Screening	Scanning Location	Non-Intrusive Container Screening	% Screening	Intrusive Container Screening	Screening requirements	Data Sharing
Status Quo	None	None	None	0%	None	None	None
0% inspection	ATS (status quo)	Mobile system	Gamma ray scanners	5%	Human	Containers that don't pass the non-intrusive inspection	Smart Tags
100% Inspection (100% of containers)	ATS+ (shippers submit manifests to ATS system 24 hours before ship loading)	On crane spreaders	X-ray scanners	25%	Animals	Random (fixed percentage)	Upload container screening data to destination port
Improved loading search		Fixed entry point with truck drive-through	Operator experience	50%	Portable Radiation Detectors	Containers tagged high risk by manifest screening	
Minimize port operations disruption			Trained animals	75%	Remotely-operated inspection robots	100%	
High Performance			Radiation detectors	100%			
100% Intrusive Inspection			Scales				

Alternative	eScales	eAnimals	eRad	eGamma	
5	No	No	No	No	
	hRad	hGamma			
	No	No			
	iAnimals	iRad	iGamma	iBio	iChem
	Yes	Yes	Yes	Yes	Yes
	cScales	cRad	cGamma		
	No	No	No		
	ATS	eScanPrc	iRdmSelPrc		
	None	0%	100%		

Figure H6. Experiment Configuration of Alternative 5

The last alternative, “100% Intrusive Inspection”, is a brute-force solution by examining every container that passes through the port. While it is expectedly resource consuming and productivity-stopping, it is still interesting to model it to compare its performance with the alternatives. This alternative includes a comprehensive sensor suite of trained animals, radiation detectors, biological detectors and chemical detectors for the intrusive inspection team. Since all containers are intrusively inspection, there is no need for ATS risk profiling.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX I: SSTG MODEL DATA ANALYSIS SUPPLEMENT

1) Logistic Regression Model and S-Plus output for basic model without 2-way interactions.

```

*** Generalized Linear Model ***

Call: glm(formula = Detected ~ eScales + eAnimals + eRad + eGamma + hRad
+ hGamma + iAnimals + iRad + iGamma + iBio + iChem + cScales + cRad + cGamma +
ATS +
      eScanPrc + iRdmSelPrc, family = binomial(link = logit), data =
IPDataAnalysis.25May07., na.action = na.exclude, control = list(epsilon =
0.0001,
      maxit = 50, trace = F))
Deviance Residuals:
      Min       1Q   Median       3Q      Max
-3.1105 -0.7095312  0.4073242  0.7620027  2.209216

Coefficients:
              Value Std. Error    t value
(Intercept) -3.098069316  0.15530329 -19.9485111
      eScales  0.035894339  0.06052711  0.5930291
      eAnimals  0.038208799  0.05860065  0.6520200
        eRad  0.022254942  0.05879198  0.3785371
      eGamma  0.220332374  0.06440027  3.4212957
        hRad  0.286455958  0.06152093  4.6562361
      hGamma  1.237160697  0.06070090  20.3812588
      iAnimals  1.298526573  0.06248584  20.7811330
        iRad  0.489334406  0.05950026  8.2240724
      iGamma  1.586675979  0.06197039  25.6037767
        iBio  0.397018826  0.05908367  6.7196038
        iChem  0.317137116  0.06014602  5.2727866
      cScales  0.099687004  0.05877058  1.6962058
        cRad  0.009215452  0.05866183  0.1570945
      cGamma  1.931360243  0.06556379  29.4577271
        ATS -0.086769601  0.04184448 -2.0736211
      eScanPrc  0.193242236  0.09388888  2.0582014
      iRdmSelPrc -0.308788933  1.03856075 -0.2973239

(Dispersion Parameter for Binomial family taken to be 1 )

Null Deviance: 10028.47 on 7786 degrees of freedom

Residual Deviance: 7512.23 on 7769 degrees of freedom

Number of Fisher Scoring Iterations: 4

Analysis of Deviance Table

Binomial model

Response: Detected

```

Terms added sequentially (first to last)

	Df	Deviance	Resid. Df	Resid. Dev
NUL			7786	10028.47
eScales	1	2.247	7785	10026.22
eAnimals	1	0.112	7784	10026.11
eRad	1	1.413	7783	10024.70
eGamma	1	3.362	7782	10021.34
hRad	1	8.744	7781	10012.59
hGamma	1	316.130	7780	9696.46
iAnimals	1	324.847	7779	9371.62
iRad	1	69.160	7778	9302.46
iGamma	1	643.163	7777	8659.29
iBio	1	44.175	7776	8615.12
iChem	1	3.715	7775	8611.40
cScales	1	0.871	7774	8610.53
cRad	1	0.731	7773	8609.80
cGamma	1	1087.109	7772	7522.69
ATS	1	6.046	7771	7516.64
eScanPrc	1	4.327	7770	7512.32
iRdmSelPrc	1	0.088	7769	7512.23
iGamma	1	641.895	7775	8658.30
iBio	1	44.093	7774	8614.21
iChem	1	3.597	7773	8610.61
cScales	1	0.753	7772	8609.86
cRad	1	0.663	7771	8609.20
cGamma	1	1087.070	7770	7522.13
ATS	1	6.092	7769	7516.03
eScanPrc	1	4.634	7768	7511.40
iRdmSelPrc	1	0.085	7767	7511.32

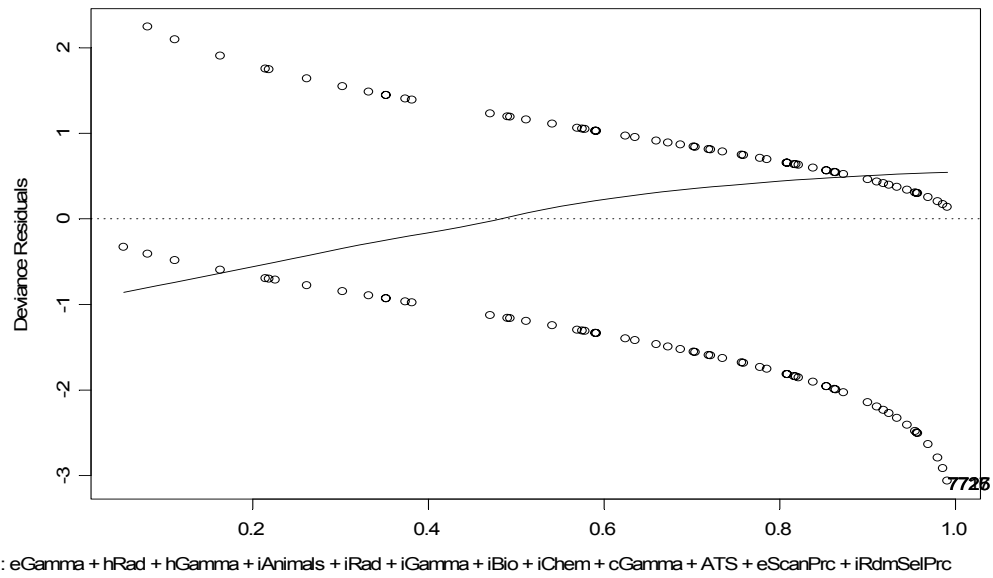
2) Logistic Regression Model output from Minitab

Logistic Regression Table

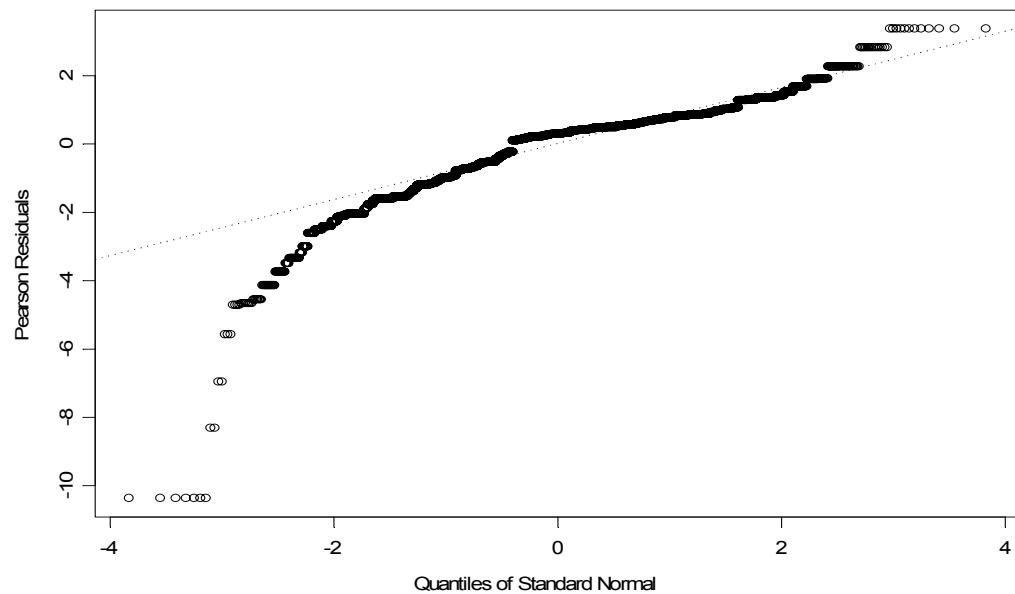
Predictor	Coef	SE Coef	Z	P	Odds Ratio	95% CI	
						Lower	Upper
Constant	-3.09808	0.155474	-19.93	0.000			
eScales	0.0358970	0.0605623	0.59	0.553	1.04	0.92	1.17
eAnimals	0.0382102	0.0586279	0.65	0.515	1.04	0.93	1.17
eRad	0.0222567	0.0588220	0.38	0.705	1.02	0.91	1.15
eGamma	0.220334	0.0644292	3.42	0.001	1.25	1.10	1.41
hRad	0.286458	0.0615533	4.65	0.000	1.33	1.18	1.50
hGamma	1.23716	0.0607261	20.37	0.000	3.45	3.06	3.88
iAnimals	1.29853	0.0625399	20.76	0.000	3.66	3.24	4.14
iRad	0.489337	0.0595368	8.22	0.000	1.63	1.45	1.83
iGamma	1.58668	0.0620209	25.58	0.000	4.89	4.33	5.52
iBio	0.397020	0.0591111	6.72	0.000	1.49	1.32	1.67
iChem	0.317141	0.0601905	5.27	0.000	1.37	1.22	1.55
cScales	0.0996895	0.0588044	1.70	0.090	1.10	0.98	1.24
cRad	0.0092159	0.0586880	0.16	0.875	1.01	0.90	1.13
cGamma	1.93137	0.0656199	29.43	0.000	6.90	6.07	7.85
ATS	-0.0867702	0.0418620	-2.07	0.038	0.92	0.84	1.00
eScanPrc	0.193241	0.0939325	2.06	0.040	1.21	1.01	1.46
iRdmSel	-0.308825	1.03912	-0.30	0.766	0.73	0.10	5.63

3) Graphs

a) Residual Deviance

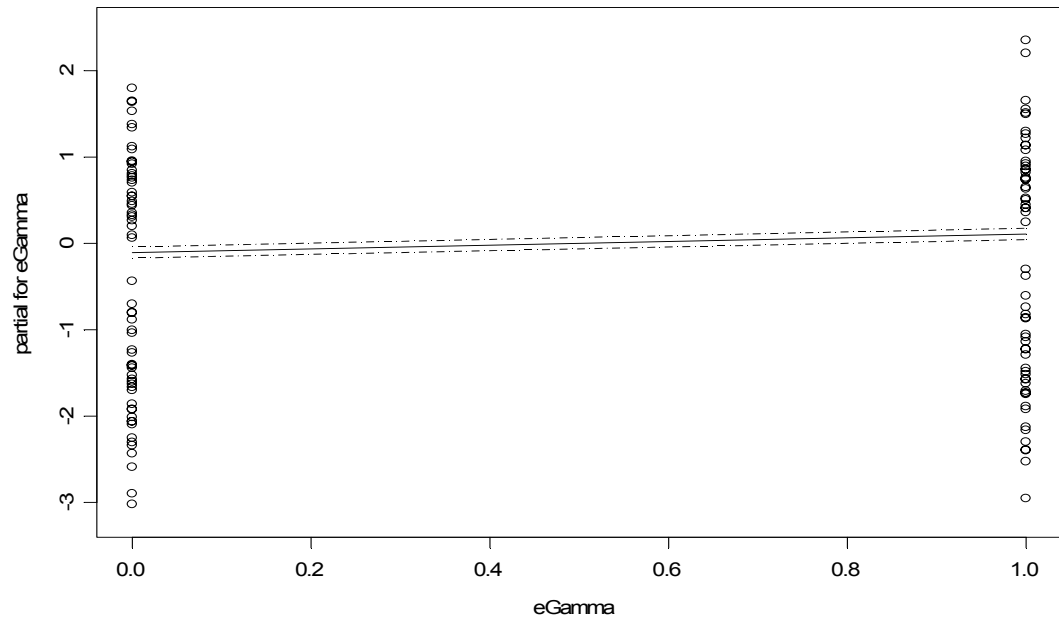


b) Normal QQ Plot

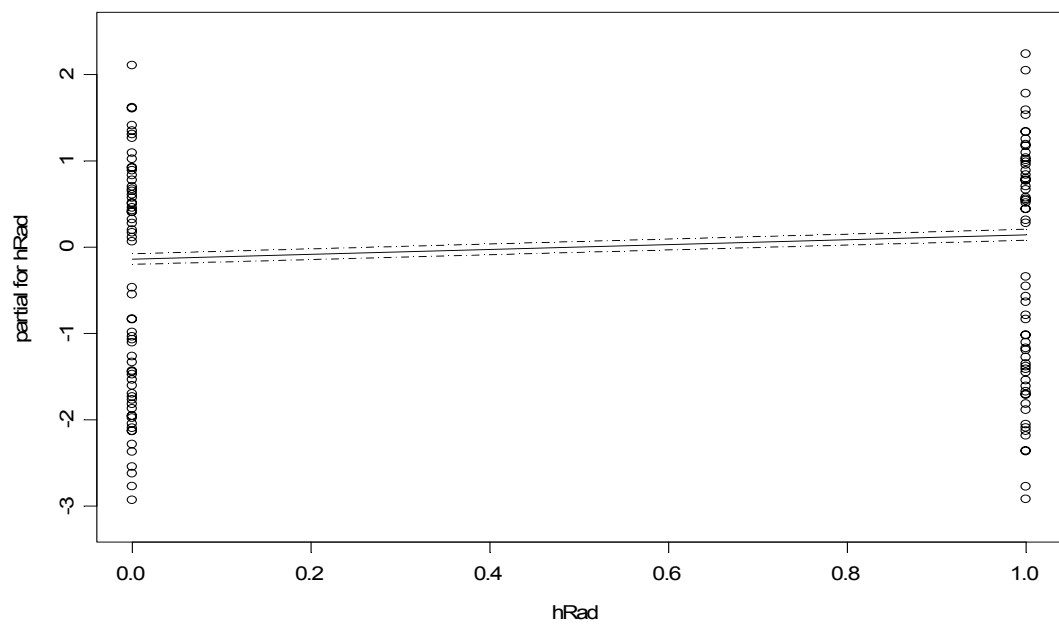


c) **Partial Fit Plots**

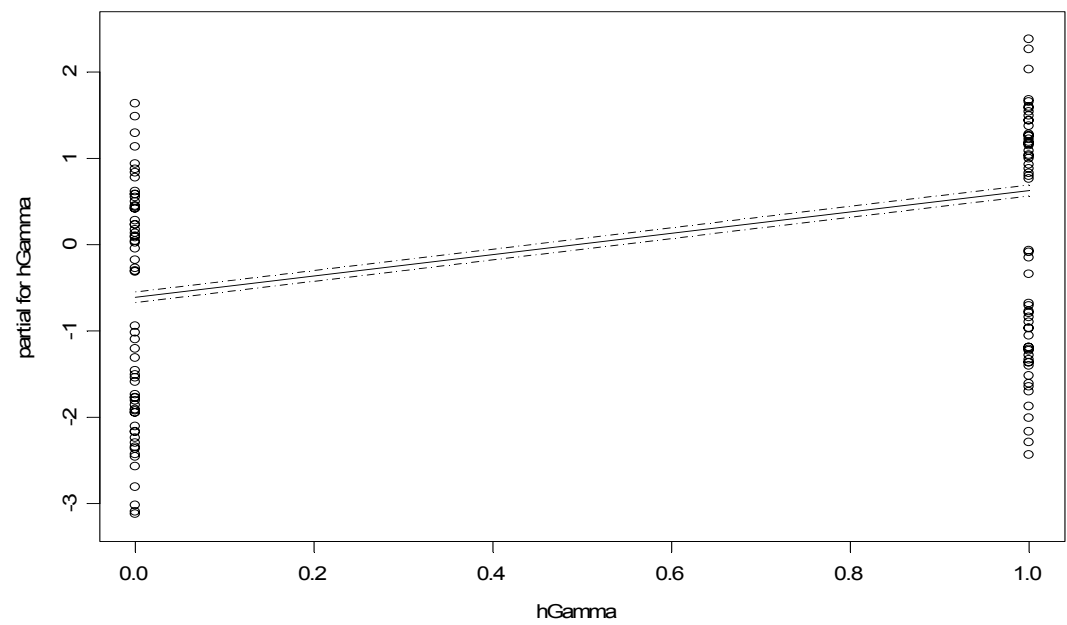
i) **Gamma Scanner at Port of Entry**



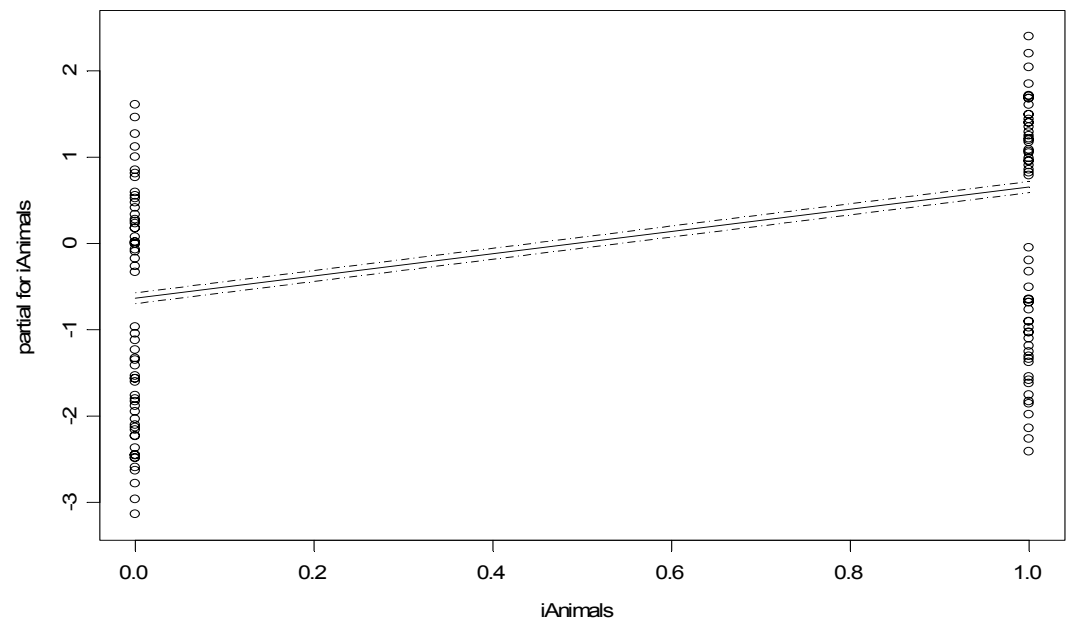
ii) **Radiation Detector at the Holding Area**



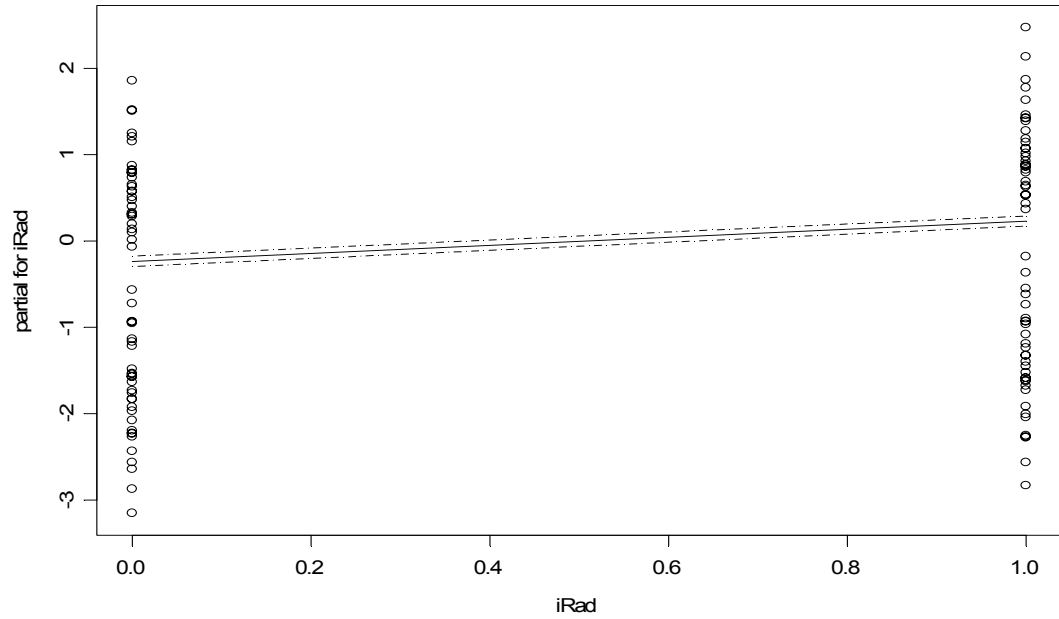
iii) Gamma Detector at the Holding Area



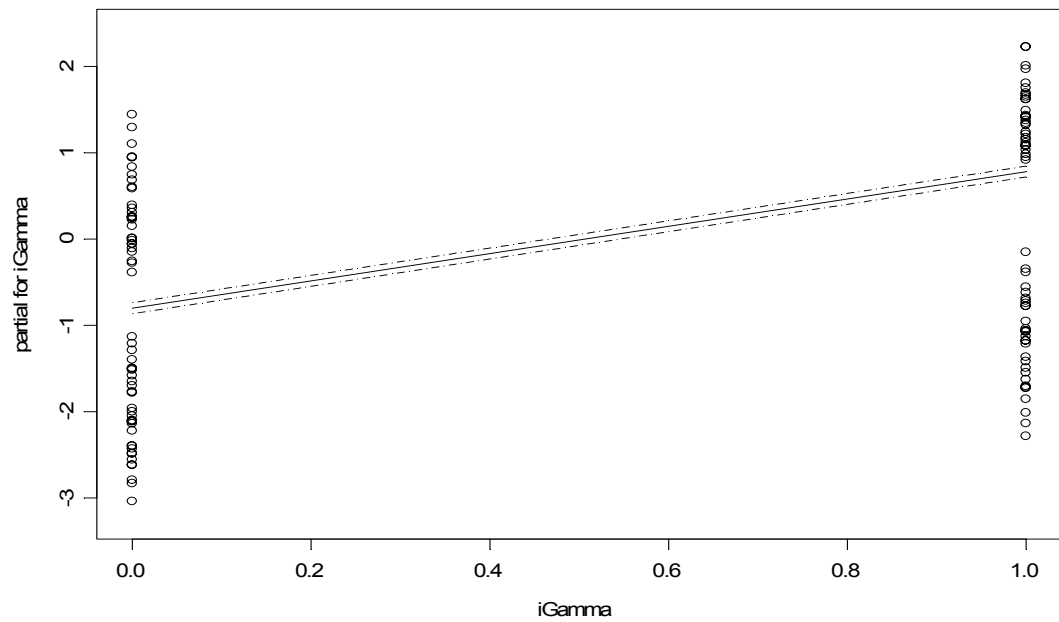
iv) Animals at the Inspection Station



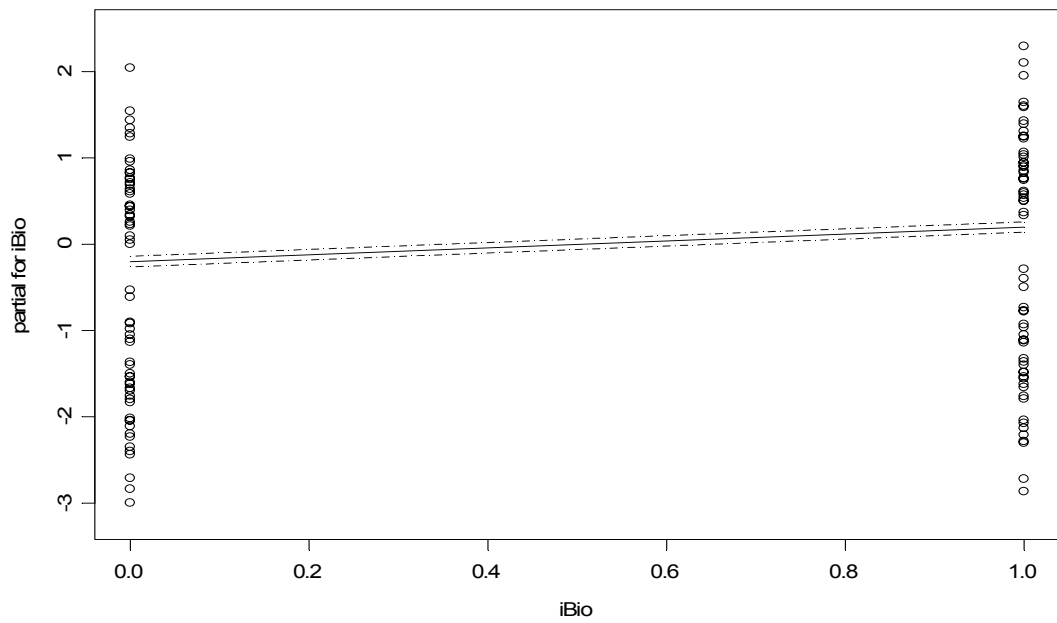
v) **Radiation Detector at the Inspection Station**



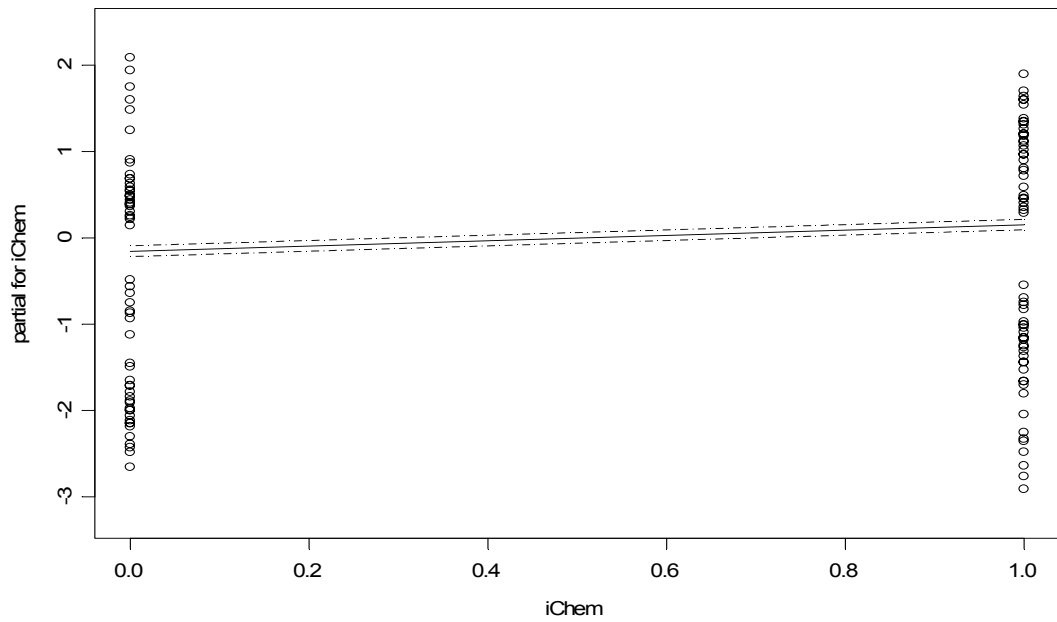
vi) **Gamma Detector at the Inspection Station**



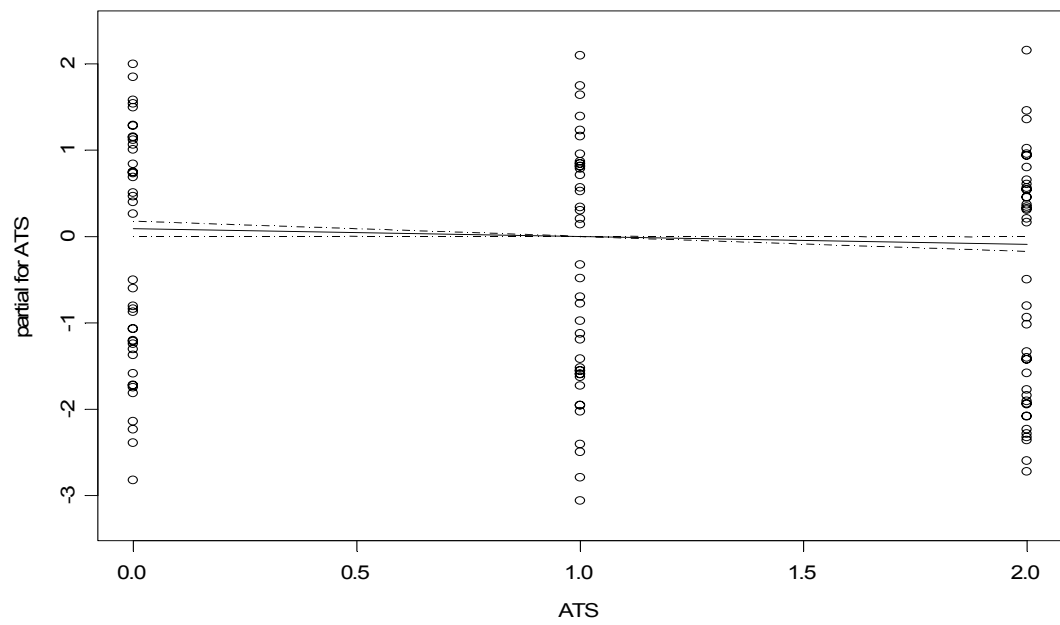
vii) Biological Scanner at the Inspection Station



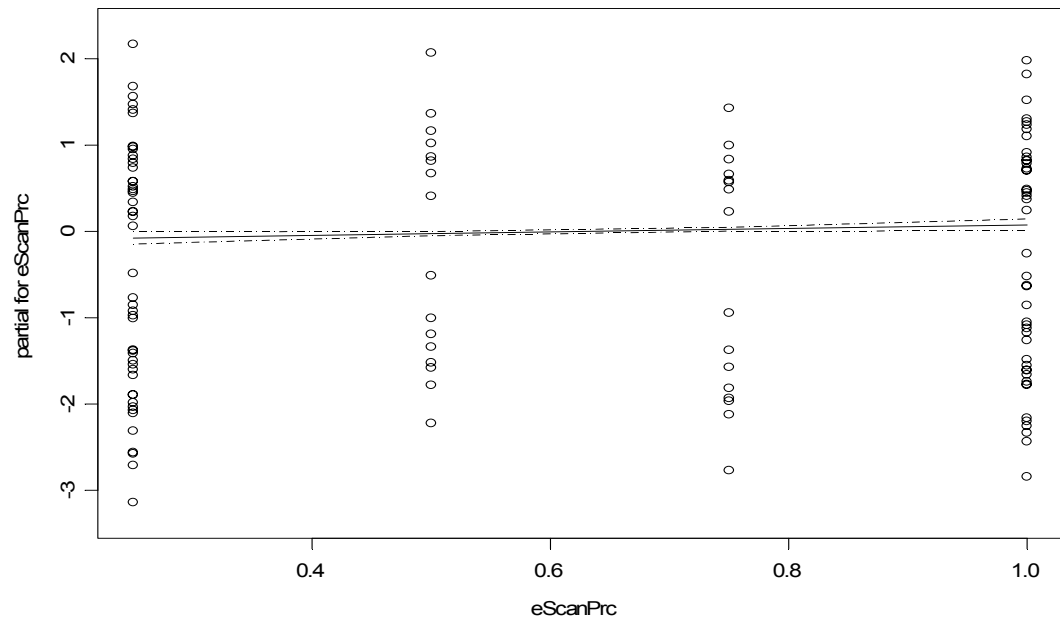
viii) Chemical Detector at the Inspection Station



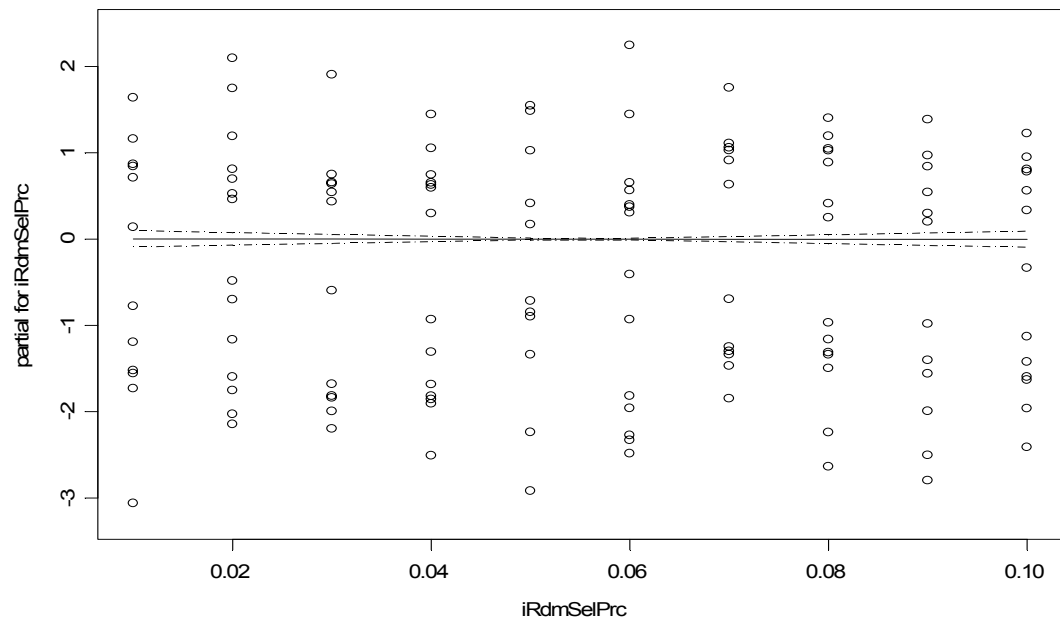
ix) ATS



x) Scanning Percentage at the Port of Entry (Truck Scanning Station)



xi) **Random Scanning Selection Percentage**



Point of Entry						Holding Area						Inspection Center						Crane Loading						Run #	Run Idx
Enter	Served	Util	Q lgth	Q time	Avg Time	Enter	Served	Util	Q lgth	Q Time	Avg Time	Enter	Served	Util	Q lgth	Q time	Avg Time	Enter	Served	Util	Q lgth	Q Time	Avg Time	Run #	Run Idx
103	102	0.002	0.498	0	8.36	1885	1885	0.174	937.3	3721.4	1975.7	302	302	0	0.499	0	0	1987	1987	0.251	253.3	1379	1439.3	1	1
103	102	0.002	0.498	0	7.98	1885	1885	0.175	937.3	3758.4	2008.7	324	324	0	0.499	0	0	1987	1987	0.249	244.3	1325	1384.8	2	1
103	102	0.002	0.498	0	8.2	1885	1885	0.174	937.3	3709.3	1948.6	313	313	0	0.499	0	0	1987	1987	0.254	266.2	1464	1524.7	3	1
103	102	0.002	0.498	0	8.22	1885	1885	0.174	937.3	3770.3	2024.5	312	312	0	0.499	0	0	1987	1987	0.252	254.6	1393	1453	4	1
103	102	0.002	0.498	0	8	1885	1885	0.173	937.3	3725.5	1980.6	319	319	0	0.499	0	0	1987	1987	0.252	258	1413	1473.8	5	1
103	102	0.002	0.498	0	8.1	1885	1885	0.174	937.3	3743.1	1997.5	345	345	0	0.499	0	0	1987	1987	0.251	248.4	1354	1413.6	6	1
103	102	0.002	0.498	0	8.26	1885	1885	0.173	937.3	3720.1	1971.8	319	319	0	0.499	0	0	1987	1987	0.25	252.4	1372	1431.6	7	1
103	102	0.002	0.498	0	7.36	1885	1885	0.173	937.3	3743.8	2000.2	305	305	0	0.499	0	0	1987	1987	0.253	254.5	1399	1459.7	8	1
103	102	0.002	0.498	0	8.49	1885	1885	0.174	937.3	3730.8	1980.2	291	291	0	0.499	0	0	1987	1987	0.253	256.5	1408	1468.6	9	1
103	102	0.002	0.498	0	8.32	1885	1885	0.174	937.3	3751.2	1999	315	315	0	0.499	0	0	1987	1987	0.252	254	1382	1442	10	1
103	102	0.002	0.498	0	8.2	1885	1885	0.174	937.3	3771.6	2024.5	312	310	0.872	110.1	13191.8	13093.5	1896	1896	0.24	113.6	624	684.15	1	2
103	102	0.002	0.498	0	7.88	1885	1885	0.173	937.3	3719.6	1985.5	329	328	0.915	122.2	14539.7	16385.8	1894	1894	0.241	109.9	611.2	671.81	2	2
103	102	0.002	0.498	0	8.25	1885	1885	0.175	937.3	3789.9	2037.1	338	338	0.932	120.5	14430.3	16217.7	1909	1909	0.241	91.94	501.8	561.87	3	2
103	102	0.002	0.498	0	7.92	1885	1885	0.174	937.3	3750.4	2016.1	303	302	0.847	106.2	13031.6	14889.8	1901	1901	0.239	116.2	629.7	689.56	4	2
103	102	0.002	0.498	0	7.68	1885	1885	0.174	937.3	3711.1	1965.8	340	340	0.936	125.7	15035.7	16819	1891	1891	0.236	99.49	537.8	597.17	5	2
103	102	0.002	0.498	0	7	1885	1885	0.174	937.3	3719.3	1985.8	328	328	0.898	122.4	14541.2	16315.4	1899	1899	0.241	110.4	604.3	664.67	6	2
103	102	0.002	0.498	0	8.5	1885	1885	0.175	937.3	3754	1994	341	340	0.948	121.9	14648.9	16496.8	1890	1890	0.238	93.58	507.3	567.14	7	2
103	102	0.002	0.498	0	9.09	1885	1885	0.173	937.3	3705.2	1967	295	294	0.83	102.8	12701.6	14569.2	1899	1899	0.24	124.3	677.1	737.19	8	2
103	102	0.002	0.498	0	7.51	1885	1885	0.174	937.3	3765.5	2011.3	305	305	0.827	104.9	12223.1	13980.2	1892	1892	0.237	98.37	538.7	598.27	9	2
103	102	0.002	0.498	0	7.45	1885	1885	0.175	937.3	3763.9	2006.7	330	329	0.937	123.2	15324.2	17213.2	1906	1906	0.238	83.03	450.4	509.81	10	2
103	102	0.002	0.498	0	8.54	1885	1885	0.176	937.3	3792.2	2037.1	455	363	0.997	185.3	17615.4	18636.1	1979	1978	0.25	86.28	473.4	533.73	1	3
103	102	0.002	0.498	0	7.73	1885	1885	0.174	937.3	3754.8	2002	444	355	0.997	179.9	17585.1	18630.2	1977	1977	0.249	98.87	537	596.97	2	3
103	102	0.002	0.498	0	7.74	1885	1885	0.176	937.3	3795.6	2032	432	356	0.998	172.5	17389.9	18425.9	1980	1978	0.247	97.15	523.2	582.99	3	3
103	102	0.002	0.498	0	7.84	1885	1885	0.176	937.3	3778.7	2004.9	427	350	0.996	177	17662.3	18718	1979	1977	0.246	89.96	487.7	547.38	4	3
103	102	0.002	0.498	0	7.1	1885	1885	0.175	937.3	3762.2	2004.6	453	357	0.997	186.8	17453.7	18480.1	1955	1955	0.246	86.24	468.8	528.5	5	3
103	102	0.002	0.498	0	8.31	1885	1885	0.176	937.3	3822	2055.9	424	344	0.997	176	17657.6	18735.5	1970	1969	0.248	87.91	478.5	538.54	6	3
103	102	0.002	0.498	0	8.22	1885	1885	0.175	937.3	3797.8	2032.6	437	343	0.995	183.1	17495.2	18545.1	1957	1957	0.251	94.65	526.4	587.32	7	3
103	102	0.002	0.498	0	8.22	1885	1885	0.175	937.3	3778.6	2022.4	442	344	0.996	184.3	17226.5	18267.2	1958	1957	0.247	90.86	498.6	558.86	8	3
103	102	0.002	0.498	0	7.9	1885	1885	0.173	937.3	3728.9	2003.5	438	346	0.995	180.3	17683.2	18738.5	1972	1972	0.249	100.3	545.1	605.01	9	3
103	102	0.002	0.498	0	7.85	1885	1885	0.174	937.3	3736.6	1985	428	362	0.996	178.8	18023.2	19053.1	1971	1970	0.246	93.69	507.8	567.52	10	3
103	102	0.002	0.498	0	8.64	1885	1885	0.176	937.3	3811.5	2045.6	390	359	0.996	138	16573.5	17799.2	1978	1978	0.247	110	591.2	650.57	1	4
103	102	0.002	0.498	0	8.26	1885	1885	0.173	937.3	3746.1	1999.9	390	344	0.995	152.4	17187.9	18349.1	1955	1955	0.247	113.4	616.8	676.87	2	4
103	102	0.002	0.498	0	7.28	1885	1885	0.174	937.3	3750.5	1994.1	381	350	0.995	144.3	16911.7	18026.2	1934	1934	0.243	103.1	564.6	624.31	3	4

103	102	0.002	0.498	0	7.58	1885	1885	0.175	937.3	3745.8	1994	395	352	0.996	154.1	17040	18159.5	1944	1944	0.246	115.4	630.3	690.42	4	4
103	102	0.002	0.498	0	8.83	1885	1885	0.175	937.3	3768.8	2020.6	406	366	0.996	159.6	17134.4	18250.2	1950	1950	0.246	102.9	559	618.89	5	4
103	102	0.002	0.498	0	8.71	1885	1885	0.174	937.3	3719.4	1977.1	376	344	0.995	143.3	17100	18231.8	1940	1939	0.244	115	624.7	684.87	6	4
103	102	0.002	0.498	0	7.9	1885	1885	0.174	937.3	3749.7	1994.8	365	357	0.99	133.5	16113	17736.4	1973	1973	0.248	114.6	622.8	682.61	7	4
103	102	0.002	0.498	0	8.23	1885	1885	0.176	937.3	3772.5	2013	423	347	0.996	169	16948.8	18005.8	1939	1939	0.245	101.7	554	614.03	8	4
103	102	0.002	0.498	0	8.92	1885	1885	0.176	937.3	3768.1	2011.5	415	352	0.997	164.7	17269.4	18350.7	1935	1935	0.243	107.7	583.1	642.76	9	4
103	102	0.002	0.498	0	8.44	1885	1885	0.174	937.3	3731.9	1978.7	379	345	0.996	136.6	16402.1	17655.7	1984	1983	0.248	131	707.4	767.31	10	4
103	102	0.002	0.498	0	7.61	1885	1885	0.175	937.3	3763.3	2012	285	285	0.825	99.95	12683	14557.7	2027	2027	0.257	149	813.9	874.19	1	5
103	102	0.002	0.498	0	8.1	1885	1885	0.174	937.3	3754.2	2016	306	305	0.83	102.5	11967.2	13766.8	2029	2029	0.256	143.9	789.6	849.67	2	5
103	102	0.002	0.498	0	8.45	1885	1885	0.174	937.3	3738.5	1990.2	303	303	0.861	103.9	12849.4	14691.3	2026	2026	0.255	143.1	772.7	832.62	3	5
103	102	0.002	0.498	0	8.2	1885	1885	0.173	937.3	3720.2	1986.9	290	290	0.794	99.17	11744.9	13519.5	2032	2032	0.255	152.6	830.2	889.91	4	5
103	102	0.002	0.498	0	7.69	1885	1885	0.176	937.3	3783	2009.1	309	308	0.86	104.8	12914.8	14763.7	2032	2032	0.256	143.4	779.9	839.86	5	5
103	102	0.002	0.498	0	8.27	1885	1885	0.174	937.3	3774.4	2023	283	281	0.794	91.61	11257.8	13161	2021	2021	0.257	160.3	877.9	938.22	6	5
103	102	0.002	0.498	0	8.3	1885	1885	0.172	937.3	3708.2	1979.9	277	277	0.767	94.24	11359.7	13153.1	2046	2046	0.258	165.3	896	955.96	7	5
103	102	0.002	0.498	0	8.57	1885	1885	0.176	937.3	3802.7	2041.7	316	316	0.884	109	13278.4	15092.1	2052	2052	0.259	136.5	740	800.08	8	5
103	102	0.002	0.498	0	8.02	1885	1885	0.173	937.3	3711.6	1977.5	293	293	0.798	104.1	12415.6	14181	2025	2025	0.255	158.6	863.1	922.99	9	5
103	102	0.002	0.498	0	7.82	1885	1885	0.174	937.3	3750.3	2003.2	283	281	0.751	91.19	10666.7	12466.4	2031	2031	0.256	158.8	863.5	923.29	10	5
103	102	0.002	0.498	0	8.47	1885	1885	0.175	937.3	3770.3	2017.9	248	248	0.698	76.68	9434.55	11257.7	1992	1992	0.251	163	882.3	942.18	1	6
103	102	0.002	0.498	0	7.57	1885	1885	0.175	937.3	3764.9	2011.5	306	306	0.841	107.2	12603.5	14383.7	1986	1986	0.25	138.2	752.8	812.65	2	6
103	102	0.002	0.498	0	6.69	1885	1885	0.175	937.3	3767.5	2006	253	253	0.711	82.34	10146	11966	1979	1979	0.249	156.2	853.5	913.22	3	6
103	102	0.002	0.498	0	7.86	1885	1885	0.173	937.3	3717.4	1973.6	271	271	0.759	94.72	11554	13370	1976	1976	0.248	156.6	849	908.71	4	6
103	102	0.002	0.498	0	8.26	1885	1885	0.174	937.3	3762.2	2019.2	243	241	0.67	75.13	9060.07	10921.8	1987	1987	0.25	165.1	899.7	959.4	5	6
103	102	0.002	0.498	0	8.16	1885	1885	0.175	937.3	3759.5	2008.3	286	286	0.803	97.98	12014.2	13834.7	1971	1971	0.248	143.9	783.1	842.96	6	6
103	102	0.002	0.498	0	8.5	1885	1885	0.175	937.3	3753.7	2005.4	274	274	0.765	89.86	11055.4	12863.8	1975	1975	0.249	153	836	895.96	7	6
103	102	0.002	0.498	0	9.01	1885	1885	0.176	937.3	3829	2062.9	292	291	0.825	101.4	12606.8	14483.8	1987	1987	0.251	133.7	730.6	790.64	8	6
103	102	0.002	0.498	0	7.72	1885	1885	0.173	937.3	3754.4	2004	276	276	0.751	86.42	10082.7	11844.8	1986	1986	0.249	154.2	838.9	898.37	9	6
103	102	0.002	0.498	0	8.69	1885	1885	0.174	937.3	3722.7	1984.2	256	256	0.716	86.34	10585	12396.8	1981	1981	0.249	164.4	892	951.75	10	6
103	102	0.002	0.498	0	7.69	1885	1885	0.174	937.3	3751.9	2016.8	366	353	0.994	119.6	14311.1	15954.4	2110	2109	0.265	145.2	790.8	850.86	1	7
103	102	0.002	0.498	0	7.28	1885	1885	0.174	937.3	3745.2	2004.6	350	350	0.964	104.6	12349.9	14133.9	2133	2133	0.268	159.7	864.8	924.38	2	7
103	102	0.002	0.498	0	7.63	1885	1885	0.173	937.3	3715.1	1986.1	373	349	0.995	122.7	14603.1	16028.1	2115	2115	0.268	158.4	866.1	926.27	3	7
103	102	0.002	0.498	0	8.31	1885	1885	0.173	937.3	3723.5	2002.1	368	347	0.994	121.7	14466.2	15908.3	2122	2120	0.267	157.9	850.7	911.25	4	7
103	102	0.002	0.498	0	8.56	1885	1885	0.175	937.3	3768.5	2023.8	368	348	0.995	114.5	13693.8	15211.4	2127	2127	0.266	145.3	785.9	845.34	5	7
103	102	0.002	0.498	0	8.11	1885	1885	0.173	937.3	3737.7	2007.2	344	343	0.941	100.8	11964.1	13773.7	2129	2129	0.269	162.1	887.7	947.67	6	7
103	102	0.002	0.498	0	8.26	1885	1885	0.174	937.3	3763.1	2017.1	358	357	0.957	114.5	13337.9	15098.7	2129	2129	0.268	144.9	791.3	851.09	7	7
103	103	0.002	0.498	0	7.91	1885	1885	0.175	937.3	3738.4	1983.6	371	347	0.994	113.9	13818.1	15290.1	2121	2120	0.267	151.9	826.8	887.01	8	7
103	103	0.002	0.498	0	8.13	1885	1885	0.176	937.3	3798.2	2046	362	348	0.994	118.1	14664.1	16353.5	2118	2117	0.269	141.6	778.3	839.03	9	7

103	102	0.002	0.498	0	7.33	1885	1885	0.174	937.3	3749.5	2006.8	411	349	0.996	147.3	16125.4	17460	2085	2085	0.264	138.8	767.3	827.5	10	7
103	103	0	0.498	0	0	1885	1885	0.174	937.3	3763.3	2015.2	365	344	0.996	123.9	14879.5	16313.9	2044	2043	0.258	142.6	776.7	837.01	1	8
103	103	0	0.498	0	0	1885	1885	0.174	937.3	3780.1	2010.8	403	355	0.994	136.4	15016.9	16384.2	2033	2032	0.256	142.1	773.5	833.81	2	8
103	103	0	0.498	0	0	1885	1885	0.174	937.3	3762.3	2022.5	408	355	0.995	134.9	14528.3	15909.5	2029	2028	0.256	145.9	794.1	854.56	3	8
103	103	0	0.498	0	0	1885	1885	0.176	937.3	3785.7	2011.7	394	351	0.995	134.3	15323.2	16757.9	2036	2034	0.258	137.5	752.4	813.43	4	8
103	103	0	0.498	0	0	1885	1885	0.175	937.3	3773.5	2013.9	416	346	0.994	143.6	15452.3	16786.9	2019	2018	0.254	140.3	769.5	829.8	5	8
103	103	0	0.498	0	0	1885	1885	0.175	937.3	3772.9	2018.8	407	357	0.993	145.4	15654.8	16992.8	2007	2005	0.253	128.4	700.4	761.05	6	8
103	103	0	0.498	0	0	1885	1885	0.174	937.3	3753.4	2004.6	389	347	0.994	132.7	15074.2	16489.6	2041	2039	0.258	139.2	762.7	823.56	7	8
103	103	0	0.498	0	0	1885	1885	0.177	937.3	3808.1	2029.5	362	355	0.992	120	14518.9	16291.2	2056	2054	0.257	139.9	755.7	815.93	8	8
103	103	0	0.498	0	0	1885	1885	0.174	937.3	3726.8	1993.5	379	352	0.994	123.3	14564.1	15967.2	2033	2031	0.256	155.9	847.9	908.58	9	8
103	103	0	0.498	0	0	1885	1885	0.173	937.3	3733.3	1997.6	370	358	0.994	117	13803	15616.8	2055	2053	0.258	148.5	807.3	867.89	10	8
26	26	5E-04	0.491	0	8.45	1885	1885	0.176	937.3	3774.7	2021.2	414	360	0.994	150.2	16244.1	17517	2020	2019	0.252	126.7	676.2	735.72	1	9
28	28	6E-04	0.491	0	9.47	1885	1885	0.174	937.3	3745.7	2000.3	458	342	0.994	172.3	16817	18056.8	1993	1991	0.251	126.6	686.3	746.9	2	9
40	39	7E-04	0.494	0	8.07	1885	1885	0.172	937.3	3699.3	1966.1	423	345	0.996	155.1	16290.7	17574.6	2002	2002	0.252	131.1	716.2	775.85	3	9
23	22	4E-04	0.489	0	8.29	1885	1885	0.177	937.3	3822	2056.7	404	360	0.997	145	16003.1	17286	2016	2016	0.252	111.5	602.8	662.31	4	9
24	24	3E-04	0.49	0	6.1	1885	1885	0.176	937.3	3784.8	2015.6	385	357	0.995	130.8	15729.6	17073	2042	2039	0.259	129.2	719.6	780.89	5	9
30	30	6E-04	0.492	0	8.64	1885	1885	0.174	937.3	3729.7	1988.8	422	356	0.995	150.1	15795.8	17107	2032	2031	0.256	138.1	753.9	814.11	6	9
28	27	4E-04	0.491	0	6.37	1885	1885	0.173	937.3	3716.4	1970	429	344	0.997	158.1	16271.2	17545.2	2014	2013	0.253	130.4	705.4	765.43	7	9
29	29	5E-04	0.492	0	7.74	1885	1885	0.174	937.3	3744.2	1999.4	455	351	0.996	175.3	16973.1	18124.5	1978	1977	0.251	116.8	637.4	698.05	8	9
27	27	5E-04	0.491	0	7.36	1885	1885	0.174	937.3	3773.3	2030	413	341	0.996	154.7	16420	17680	2005	2003	0.253	129.8	706.4	767.22	9	9
28	28	6E-04	0.491	0	9.05	1885	1885	0.176	937.3	3791.2	2023.1	444	352	0.995	163.8	16472.6	17721.9	2005	2004	0.251	116.1	634.6	694.54	10	9
20	19	4E-04	0.488	0	8.99	1885	1885	0.175	937.3	3772.6	2021.7	537	351	0.996	232.7	18186.6	19234.8	1939	1939	0.246	82.89	454.2	514.57	1	10
30	30	6E-04	0.492	0	8.05	1885	1885	0.174	937.3	3768.2	2021	513	358	0.997	217.7	18162.9	19199.9	1954	1953	0.247	90.26	491.9	552.35	2	10
29	28	5E-04	0.492	0	7.51	1885	1885	0.173	937.3	3732.1	2001	497	349	0.997	206.7	17512.8	18555.1	1959	1959	0.247	97.83	529.7	589.61	3	10
28	28	5E-04	0.491	0	8.03	1885	1885	0.174	937.3	3754.2	2003.9	500	364	0.996	212.6	18447.1	19491.6	1981	1981	0.248	81.08	441.3	500.79	4	10
26	26	4E-04	0.491	0	6.84	1885	1885	0.173	937.3	3743.3	2003.3	499	339	0.995	208.6	17577.3	18655.4	1956	1953	0.246	98.35	532.5	593.05	5	10
36	36	7E-04	0.493	0	8.73	1885	1885	0.174	937.3	3733.2	1990.7	510	349	0.995	219	17752.1	18790.2	1930	1928	0.245	97.55	535.1	596.01	6	10
28	28	6E-04	0.491	0	9.41	1885	1885	0.175	937.3	3773	2018.2	509	350	0.997	218	17714.8	18751.3	1940	1940	0.244	84.11	453.4	513.23	7	10
27	27	6E-04	0.491	0	9.28	1885	1885	0.177	937.3	3809	2034.6	506	362	0.996	214.6	17680	18885.5	1948	1948	0.246	70.31	383.1	443.02	8	10
24	24	4E-04	0.49	0	6.49	1885	1885	0.175	937.3	3762.1	2009.5	478	345	0.996	200.3	17647.9	18705.5	1956	1955	0.245	78.69	427.5	487.28	9	10
29	28	5E-04	0.492	0	7.19	1885	1885	0.177	937.3	3793.4	2027.5	458	346	0.995	182.9	16971.9	18028.6	1992	1992	0.252	103.7	567.4	627.59	10	10
25	25	4E-04	0.49	0	7.59	1885	1885	0.174	937.3	3737.4	1990.3	387	333	0.995	162	17780.7	18883.1	1913	1911	0.241	98.46	536.7	597.21	1	11
26	25	5E-04	0.491	0	8.16	1885	1885	0.174	937.3	3746.1	1989.5	441	344	0.997	191.8	18222.3	19282.5	1859	1859	0.236	80.38	444.6	504.85	2	11
29	29	5E-04	0.492	0	7.78	1885	1885	0.173	937.3	3703.6	1965.5	394	353	0.996	154.7	17553.1	18603.6	1915	1914	0.241	101	549.3	609.55	3	11
30	30	6E-04	0.492	0	8.49	1885	1885	0.175	937.3	3756.8	1998.6	396	357	0.997	156.1	17646.4	18690	1928	1925	0.243	100.1	545.1	605.9	4	11
19	19	3E-04	0.487	0	7.01	1885	1885	0.175	937.3	3753.3	2008.8	406	353	0.998	162.3	17473.3	18522.1	1909	1908	0.242	98.93	544.9	605.49	5	11

23	23	3E-04	0.489	0	6.55	1885	1885	0.176	937.3	3773.3	2013.9	423	345	0.997	174.9	17459.8	18498.7	1885	1884	0.237	80.5	438.9	498.79	6	11
21	21	4E-04	0.488	0	8.92	1885	1885	0.174	937.3	3755.3	2011.9	414	355	0.995	164.3	17086	18102.9	1926	1926	0.243	103.2	563.5	623.4	7	11
27	27	5E-04	0.491	0	7.27	1885	1885	0.174	937.3	3765.9	2021.4	409	347	0.996	159.5	17133.4	18174.8	1901	1900	0.24	97.42	535.6	595.81	8	11
29	29	6E-04	0.492	0	8.47	1885	1885	0.175	937.3	3756.6	2006.7	406	330	0.996	161.6	17443.5	18490.1	1910	1910	0.242	101.5	556.2	616.47	9	11
28	28	5E-04	0.491	0	7.99	1885	1885	0.176	937.3	3786.6	2024	453	346	0.996	196.9	17877.2	18917.9	1854	1853	0.233	70.49	383.4	443.44	10	11
21	21	3E-04	0.488	0	7.04	1885	1885	0.174	937.3	3729.7	1983.3	337	337	0.925	118.9	14285.2	16064.8	2011	2010	0.253	134.4	723.5	783.7	1	12
21	21	3E-04	0.488	0	6.28	1885	1885	0.175	937.3	3781	2026.8	309	309	0.848	106.5	12463.6	14241.1	2024	2023	0.256	144.8	795	855.51	2	12
32	32	6E-04	0.492	0	7.9	1885	1885	0.175	937.3	3745.7	1999.6	298	297	0.801	101.2	11733.8	13516.6	2003	2002	0.252	136.7	744.1	804.18	3	12
24	24	5E-04	0.49	0	9.18	1885	1885	0.174	937.3	3748.8	1998.8	334	334	0.926	120.7	14779.5	16576.6	2031	2030	0.258	143.9	793.5	854.33	4	12
25	24	6E-04	0.49	0	10.5	1885	1885	0.175	937.3	3745.6	1992.5	287	287	0.791	98.5	11643.3	13429.8	2004	2004	0.251	138.8	744.9	804.42	5	12
17	17	4E-04	0.486	0	10.2	1885	1885	0.174	937.3	3744.4	1996.8	302	301	0.853	104.1	12881.4	14754.8	2017	2016	0.254	140.2	765.8	826.16	6	12
30	29	5E-04	0.492	0	8.07	1885	1885	0.175	937.3	3755.6	2007.1	315	315	0.881	116	13929.6	15742.2	2001	2001	0.253	133.5	727.7	787.87	7	12
26	26	5E-04	0.491	0	7.66	1885	1885	0.174	937.3	3754.8	2004.9	323	323	0.901	116.9	14193.5	16000.3	2009	2008	0.253	123.5	672.9	733.08	8	12
30	29	5E-04	0.492	0	7.87	1885	1885	0.174	937.3	3749	2009.8	335	335	0.94	117.1	14272	16090.2	2029	2028	0.256	136	741.5	801.86	9	12
27	27	5E-04	0.491	0	8.26	1885	1885	0.175	937.3	3779	2028.5	325	325	0.924	120.4	15076.2	16918.2	2019	2018	0.254	127	685	745.14	10	12
23	23	4E-04	0.489	0	8.37	1885	1885	0.174	937.3	3774.6	2029.2	325	324	0.839	107.6	12418.9	14171.6	1997	1996	0.251	149	807.7	867.89	1	13
19	19	3E-04	0.487	0	7.4	1885	1885	0.175	937.3	3772.4	2006.3	299	299	0.856	99.16	12414.8	14269.9	2018	2017	0.252	145.7	785.9	845.62	2	13
21	20	3E-04	0.488	0	6.97	1885	1885	0.175	937.3	3736.5	1989.1	346	345	0.953	124.7	15186.2	17017.9	1995	1995	0.253	138.4	730.8	811.05	3	13
25	24	4E-04	0.49	0	7.53	1885	1885	0.175	937.3	3767.5	2021.3	336	335	0.965	120.9	15024.8	16935.2	2008	2008	0.253	139.1	755.9	815.79	4	13
22	22	4E-04	0.489	0	7.63	1885	1885	0.174	937.3	3730.8	1981.5	344	343	0.943	118.5	14208.7	16031.3	2022	2021	0.256	145	798.4	839.07	5	13
23	23	4E-04	0.489	0	8.3	1885	1885	0.174	937.3	3734.2	1993.5	280	279	0.777	93.06	11116	12959.9	2014	2013	0.254	162.1	885.8	946.31	6	13
26	26	6E-04	0.491	0	9.52	1885	1885	0.175	937.3	3795.1	2032.9	348	346	0.955	115.7	13902.3	15738.3	2034	2034	0.256	136.1	739.9	799.64	7	13
25	25	5E-04	0.49	0	8.13	1885	1885	0.174	937.3	3753.4	2017.3	318	317	0.872	109	13085.9	14909.7	2007	2007	0.251	155.2	836.3	895.8	8	13
30	29	6E-04	0.492	0	8.86	1885	1885	0.174	937.3	3744.9	2005	332	332	0.955	111.7	13915	15778.3	2038	2038	0.257	154	834	893.96	9	13
29	29	6E-04	0.492	0	8.39	1885	1885	0.173	937.3	3731	1983.9	294	294	0.82	102.5	12429.6	14238	2019	2018	0.254	148.2	808.6	868.78	10	13
33	33	5E-04	0.493	0	6.59	1885	1885	0.173	937.3	3725.2	1984.7	270	270	0.732	87.01	10331	12088.7	2045	2044	0.259	170	925.2	985.73	1	14
32	31	6E-04	0.492	0	8.19	1885	1885	0.174	937.3	3756.6	2004.9	256	256	0.74	84.47	10659.6	12533.6	2050	2050	0.259	168.1	921.4	981.32	2	14
22	22	3E-04	0.489	0	6.73	1885	1885	0.175	937.3	3764.2	2014.2	267	267	0.734	81.48	9908.94	11690.5	2040	2039	0.255	163.5	883.9	943.83	3	14
27	27	5E-04	0.491	0	7.89	1885	1885	0.174	937.3	3721.1	1975.4	249	249	0.693	74.11	8851.33	10653.9	2050	2049	0.26	188.6	1037	1097.7	4	14
27	27	5E-04	0.491	0	8.59	1885	1885	0.174	937.3	3730.9	1997.6	272	272	0.736	86.31	10307.2	12059.8	2064	2063	0.26	170.6	933.3	993.61	5	14
28	28	5E-04	0.491	0	7.14	1885	1885	0.172	937.3	3703	1964.5	282	282	0.787	87.53	10566.7	12374	2051	2050	0.258	178.7	976	1036.2	6	14
23	23	4E-04	0.489	0	8.03	1885	1885	0.174	937.3	3741.9	1995.7	276	276	0.769	82.84	9990.7	11795.9	2073	2072	0.262	173.5	949.5	1010.2	7	14
16	16	3E-04	0.485	0	8.11	1885	1885	0.173	937.3	3717	1982.8	285	284	0.797	86.72	10444.7	12297	2075	2074	0.263	181.8	990.1	1050.8	8	14
29	29	5E-04	0.492	0	8.14	1885	1885	0.176	937.3	3810.3	2044.4	252	252	0.691	76.3	8962	10738.5	2050	2049	0.259	171.1	934.5	994.96	9	14
22	21	4E-04	0.489	0	8.35	1885	1885	0.172	937.3	3722.5	1983.5	250	250	0.7	75.32	9312.28	11127.8	2058	2058	0.258	181.7	974.8	1034.3	10	14
19	19	3E-04	0.487	0	7.74	1885	1885	0.176	937.3	3800.5	2041.1	181	181	0.488	51.71	6067.4	7813	1942	1941	0.244	160.1	869.8	929.98	1	15

24	24	5E-04	0.49	0	8.45	1885	1885	0.175	937.3	3777.2	2027.4	161	161	0.455	39.22	4891.65	6724.14	1947	1946	0.246	178	979.2	1039.9	2	15
22	21	3E-04	0.489	0	7.05	1885	1885	0.176	937.3	3771.4	2010.1	155	155	0.437	36.82	4469.39	6297.55	1948	1948	0.246	185.6	1008	1067.5	3	15
19	19	4E-04	0.487	0	8.76	1885	1885	0.175	937.3	3747.7	1995	202	202	0.569	63.08	7938.56	9765.44	1936	1935	0.246	162.6	895.3	956.14	4	15
25	24	4E-04	0.49	0	7.53	1885	1885	0.173	937.3	3743.9	2006	156	156	0.443	40.84	5156.27	6994.7	1947	1947	0.247	186.6	1023	1083.7	5	15
34	34	6E-04	0.493	0	8.17	1885	1885	0.174	937.3	3757.8	2012.8	184	184	0.485	54	6197.32	7904.65	1943	1942	0.247	165.2	913.7	974.73	6	15
25	25	5E-04	0.49	0	9.09	1885	1885	0.175	937.3	3755.2	2011.5	173	173	0.472	47.1	5718.68	7486.56	1946	1945	0.244	175.1	948.5	1008.6	7	15
24	24	4E-04	0.49	0	7.42	1885	1885	0.175	937.3	3752.4	1994.9	165	165	0.448	41.39	4927.57	6687.07	1951	1950	0.248	186.9	1026	1087.2	8	15
28	28	5E-04	0.491	0	7.41	1885	1885	0.176	937.3	3792.8	2025.6	152	151	0.425	35.95	4472.29	6326.8	1943	1943	0.246	178.6	979.7	1039.9	9	15
28	28	5E-04	0.491	0	7.13	1885	1885	0.175	937.3	3795	2042.4	165	165	0.457	42.19	5010.83	6806.01	1951	1950	0.247	173.8	947	1007.6	10	15
25	25	0	0.49	0	0	1885	1885	0.175	937.3	3801.3	2035.4	214	214	0.62	69.01	8612.16	10488.2	1976	1975	0.249	149.5	816.2	876.6	1	16
25	25	0	0.49	0	0	1885	1885	0.174	937.3	3758.7	2009.3	242	242	0.71	84.96	10719.7	12620.7	1972	1971	0.248	137	746.3	806.42	2	16
20	20	0	0.488	0	0	1885	1885	0.175	937.3	3765.4	2011.7	235	235	0.636	76.47	8806.79	10559.2	1971	1970	0.249	143.9	785.1	845.51	3	16
29	29	0	0.492	0	0	1885	1885	0.176	937.3	3790	2035.9	242	241	0.701	81.72	10174.5	12096.5	1973	1972	0.246	128.6	689.1	748.82	4	16
22	22	0	0.489	0	0	1885	1885	0.173	937.3	3755	2007.8	219	219	0.582	66.71	7651.3	9372.36	1977	1976	0.25	161.5	882.7	943.19	5	16
29	29	0	0.492	0	0	1885	1885	0.175	937.3	3778.1	2020.1	228	228	0.627	71.96	8858.73	10639.9	1975	1974	0.247	140	762.1	821.93	6	16
22	22	0	0.489	0	0	1885	1885	0.174	937.3	3761.3	2013.2	207	207	0.575	62.91	7459.01	9280.53	1975	1974	0.25	167.7	918.6	979.26	7	16
18	18	0	0.486	0	0	1885	1885	0.173	937.3	3735.6	1989.4	226	226	0.638	72.18	8812.83	10643.2	1980	1979	0.248	143.5	778.9	838.89	8	16
22	22	0	0.489	0	0	1885	1885	0.174	937.3	3757.7	2000.8	212	211	0.625	70.14	8857.27	10809.3	1974	1973	0.249	149.5	814	874.46	9	16
24	24	0	0.49	0	0	1885	1885	0.173	937.3	3720.4	1994.2	210	209	0.589	63.26	7768.73	9626.68	1978	1977	0.251	173.8	945.7	1006.5	10	16
53	52	1E-03	0.495	0	8.24	1885	1885	0.175	937.3	3750.4	1994.6	189	189	0.516	42.63	5108.57	6876.22	1986	1986	0.251	186.6	1024	1083.7	1	17
45	45	9E-04	0.495	0	8.72	1885	1885	0.174	937.3	3742.4	2004.2	183	183	0.5	47.76	5879.7	7651.25	1979	1978	0.251	184.7	1015	1075.9	2	17
50	50	9E-04	0.495	0	7.81	1885	1885	0.173	937.3	3724.7	1999.1	169	168	0.458	42.04	4922.12	6716.96	1980	1980	0.25	185.9	1014	1074	3	17
56	56	0.001	0.496	0	7.8	1885	1885	0.176	937.3	3778	2017.6	181	180	0.5	50.78	6172.47	7997.85	1985	1984	0.25	176.4	957.6	1018	4	17
51	50	1E-03	0.495	0	8.39	1885	1885	0.175	937.3	3784.9	2028.2	182	182	0.501	47.11	5380.28	7162.56	1981	1981	0.251	176.3	963.6	1023.7	5	17
56	56	9E-04	0.496	0	7.16	1885	1885	0.174	937.3	3761.2	2014.9	190	190	0.516	54.34	6461.84	8222.05	1982	1981	0.251	171.5	939.4	1000	6	17
50	50	0.001	0.495	0	8.85	1885	1885	0.174	937.3	3748.2	2006.1	194	193	0.518	56.13	6459.71	8224.1	1984	1983	0.251	167.2	920.8	981.4	7	17
52	52	9E-04	0.495	0	7.8	1885	1885	0.174	937.3	3737.5	1994.5	190	189	0.527	48.62	5729.68	7559.99	1980	1979	0.251	180.8	987.4	1048.2	8	17
67	66	0.001	0.496	0	7.9	1885	1885	0.174	937.3	3766.1	2009	177	177	0.507	47.27	5910.29	7768.19	1979	1979	0.249	176.4	956.7	1016.4	9	17
53	52	0.001	0.495	0	8.75	1885	1885	0.176	937.3	3781.1	2016.7	185	184	0.525	50.95	6260.66	8141.13	1974	1974	0.249	169.2	923.6	983.48	10	17
50	50	8E-04	0.495	0	7.03	1885	1885	0.175	937.3	3770.8	2010.3	305	305	0.852	111.3	13294.1	15103.5	1915	1914	0.242	110.9	604.7	665.17	1	18
59	59	0.001	0.496	0	8.32	1885	1885	0.176	937.3	3807	2035.9	300	300	0.847	108.2	13483.6	15313.2	1925	1924	0.244	109.1	596.6	657.1	2	18
56	55	0.001	0.496	0	8.69	1885	1885	0.174	937.3	3771.6	2025.8	291	290	0.799	103.9	12165.4	13991.1	1911	1911	0.242	112.6	618.9	679.09	3	18
47	46	8E-04	0.495	0	7.65	1885	1885	0.176	937.3	3782.7	2023.7	310	310	0.846	113.7	13377.1	15145.6	1923	1923	0.243	103.7	564.5	624.57	4	18
49	48	0.001	0.495	0	9.31	1885	1885	0.176	937.3	3786.3	2012.4	328	328	0.912	117	14524.1	16326.2	1921	1921	0.244	103.5	563.9	624.18	5	18
57	56	0.001	0.496	0	8.91	1885	1885	0.174	937.3	3746.1	2003.5	340	338	0.967	124.9	15413.9	17348.2	1883	1883	0.238	100.7	552.5	612.5	6	18
45	44	8E-04	0.495	0	7.87	1885	1885	0.172	937.3	3735.2	2008.4	343	341	0.973	129.2	15937.7	17848.5	1910	1910	0.24	98.32	534.2	594.04	7	18

57	57	0.001	0.496	0	7.63	1885	1885	0.173	937.3	3730.4	1993.6	310	308	0.849	109.4	12757.1	14621.1	1923	1922	0.243	123.7	678.2	738.53	8	18
47	46	9E-04	0.495	0	8.21	1885	1885	0.175	937.3	3768.4	2006	313	313	0.845	112.6	13017.7	14767.1	1916	1916	0.244	117.8	644.1	704.72	9	18
58	57	0.001	0.496	0	8.04	1885	1885	0.173	937.3	3731.8	2000.8	346	346	0.951	126.2	14940.7	16721.8	1895	1895	0.24	111.2	605.9	666.07	10	18
49	49	1E-03	0.495	0	8.69	1885	1885	0.175	937.3	3733.8	1984.5	415	355	0.997	169	17478.2	18519.9	1971	1970	0.248	106.8	583.9	644.01	1	19
44	44	0.001	0.494	0	9.83	1885	1885	0.174	937.3	3748.1	1996.5	411	354	0.995	164	17419.4	18462	1969	1968	0.248	102.3	558.2	618.36	2	19
54	54	9E-04	0.495	0	7.4	1885	1885	0.175	937.3	3778.5	2026.8	396	357	0.996	149.2	16800.5	17935	2011	2010	0.258	124.9	690.3	751.52	3	19
50	49	0.001	0.495	0	8.86	1885	1885	0.174	937.3	3738.5	1998.3	419	354	0.995	171.1	17415.4	18448	1962	1961	0.248	95.23	519.2	579.54	4	19
47	46	9E-04	0.495	0	8.58	1885	1885	0.175	937.3	3758.9	2004.6	440	355	0.998	178.9	17677.6	18738	1971	1971	0.25	117.6	642	702.31	5	19
48	48	0.001	0.495	0	9.04	1885	1885	0.176	937.3	3786.3	2038.1	389	349	0.996	152	17564.9	18701.9	1991	1989	0.251	113	616.2	676.9	6	19
45	45	8E-04	0.495	0	7.89	1885	1885	0.176	937.3	3777.6	2018.1	392	360	0.995	146.5	17066.7	18168.2	1984	1982	0.25	112.7	615.5	676.09	7	19
62	61	0.001	0.496	0	7.44	1885	1885	0.176	937.3	3780.3	2014	393	347	0.996	157	17679.4	18763.2	1983	1983	0.25	103.9	563.4	623.28	8	19
52	52	9E-04	0.495	0	7.49	1885	1885	0.175	937.3	3752.1	2004.1	383	347	0.996	147.2	17345.3	18473.4	1988	1988	0.251	109.2	594.7	654.65	9	19
50	50	9E-04	0.495	0	7.39	1885	1885	0.174	937.3	3737.4	1999.9	403	354	0.996	156.2	16813.1	17929.9	1999	1997	0.253	124.2	688.4	749.39	10	19
62	61	0.001	0.496	0	8.05	1885	1885	0.176	937.3	3793.4	2019.4	169	169	0.484	26.04	3240.17	5094.53	2056	2056	0.259	227.5	1233	1292.8	1	20
49	49	0.001	0.495	0	9.24	1885	1885	0.175	937.3	3773.2	2013.9	186	186	0.523	34.24	4172.97	5996.27	2065	2064	0.26	229.7	1249	1309.1	2	20
53	52	0.001	0.495	0	8.48	1885	1885	0.174	937.3	3738.6	1991.9	190	189	0.542	32.33	3969.68	5840.58	2057	2057	0.261	236.1	1290	1349.9	3	20
56	55	0.001	0.496	0	8.46	1885	1885	0.174	937.3	3739.2	1982.7	197	197	0.53	29.58	3442.16	5184.57	2076	2076	0.262	227.4	1240	1300	4	20
48	48	9E-04	0.495	0	8.25	1885	1885	0.175	937.3	3782.6	2034.2	165	164	0.465	25.87	3172.21	5020.28	2054	2053	0.259	217.6	1196	1256.5	5	20
51	50	8E-04	0.495	0	7.19	1885	1885	0.174	937.3	3725.7	1973.9	177	177	0.491	31.54	3829.02	5627.95	2056	2056	0.261	234	1276	1336	6	20
46	46	9E-04	0.495	0	8.28	1885	1885	0.175	937.3	3765.9	2013	174	174	0.474	34.56	4083.91	5848.36	2053	2052	0.26	225.6	1236	1296.6	7	20
49	49	0.001	0.495	0	9.52	1885	1885	0.175	937.3	3754.7	2010.5	159	157	0.426	25.01	2904.44	4680.98	2041	2040	0.257	220.1	1200	1280.2	8	20
55	55	0.001	0.495	0	7.92	1885	1885	0.174	937.3	3747	1994.8	195	195	0.545	40.09	4902.87	6714.18	2057	2056	0.26	223.2	1219	1279.8	9	20
53	53	0.001	0.495	0	9.48	1885	1885	0.173	937.3	3744.9	2004.5	170	170	0.472	31.92	3769.8	5570.31	2055	2054	0.257	217.2	1177	1237.2	10	20
44	44	7E-04	0.494	0	7.1	1885	1885	0.175	937.3	3786.2	2023.2	355	345	0.992	125.9	15525.6	17423.9	2007	2006	0.255	126.8	696	756.8	1	21
55	55	0.001	0.495	0	9.36	1885	1885	0.175	937.3	3766.9	2004.7	352	339	0.996	129.1	16169.6	18230.6	1995	1994	0.253	125.4	683.2	743.91	2	21
61	60	0.001	0.496	0	8.71	1885	1885	0.174	937.3	3779.2	2032.7	378	357	0.996	141.9	16630.2	18158	2014	2011	0.252	110.8	600.5	660.98	3	21
37	37	8E-04	0.493	0	8.82	1885	1885	0.175	937.3	3779.1	2021.3	345	343	0.941	127.5	15049.5	16907.7	2018	2017	0.255	125.5	683.1	743.57	4	21
56	56	0.001	0.496	0	9.53	1885	1885	0.175	937.3	3786.3	2023.3	345	344	0.951	126.9	15353.9	17180.5	2003	2002	0.254	120.1	653.3	713.86	5	21
52	52	9E-04	0.495	0	7.09	1885	1885	0.174	937.3	3750.9	1997.2	387	354	0.996	148.3	17129.6	18241.6	2000	1999	0.252	113.4	618	678.23	6	21
50	50	1E-03	0.495	0	8.42	1885	1885	0.174	937.3	3743.4	1999.7	382	350	0.996	149.7	17309.5	18403.8	1999	1998	0.254	114.4	627.2	687.86	7	21
47	47	8E-04	0.495	0	7.67	1885	1885	0.174	937.3	3723.9	1971	382	350	0.994	149.6	17094.6	18149.8	1982	1981	0.251	123	671.5	732.15	8	21
49	49	9E-04	0.495	0	8.38	1885	1885	0.175	937.3	3797.5	2045.4	391	348	0.995	154.5	17283.1	18336.9	1980	1980	0.25	101.4	551.2	611.28	9	21
51	50	8E-04	0.495	0	7.34	1885	1885	0.176	937.3	3780.1	2022.3	394	358	0.993	153.9	17173.2	18276.8	2008	2007	0.252	105.3	568.3	628.18	10	21
53	52	0.001	0.495	0	8.39	1885	1885	0.175	937.3	3765.9	2004.6	269	269	0.726	90.7	10586.5	12335.8	1999	1999	0.252	157.7	854.5	914.42	1	22
48	47	9E-04	0.495	0	8.44	1885	1885	0.173	937.3	3717.6	1978.8	285	285	0.8	92.29	11167.5	12967	1991	1991	0.251	165.5	898.6	958.59	2	22
55	55	0.001	0.495	0	8.87	1885	1885	0.174	937.3	3775.6	2020.3	292	292	0.83	100.1	12544.1	14387	1993	1992	0.251	149.5	818	878.22	3	22

51	51	0.001	0.495	0	8.65	1885	1885	0.175	937.3	3783.7	2030.4	296	296	0.81	98.37	11672.7	13444.9	2004	2003	0.253	145.3	798.2	858.54	4	22
48	47	9E-04	0.495	0	8.65	1885	1885	0.174	937.3	3746.3	2006.2	284	284	0.775	98.09	11495.6	13264.6	1993	1993	0.252	151.8	833.9	894.01	5	22
62	62	0.001	0.496	0	7.27	1885	1885	0.175	937.3	3766.3	2013.7	275	275	0.781	90.04	11141.1	12981.9	1993	1992	0.251	169.4	919.5	979.86	6	22
48	47	0.001	0.495	0	9.26	1885	1885	0.175	937.3	3740.4	1990.6	266	266	0.764	87.08	11041.8	12903.1	1988	1988	0.252	166	908.4	968.76	7	22
50	50	8E-04	0.495	0	6.66	1885	1885	0.174	937.3	3745.8	2006.3	271	270	0.721	81.01	9400.84	11159.8	1972	1971	0.251	165.9	913.2	974.04	8	22
52	52	0.001	0.495	0	9.13	1885	1885	0.175	937.3	3739.6	1976.6	287	287	0.784	97.26	11663.4	13433.3	1985	1984	0.249	159.2	860.5	920.6	9	22
53	53	0.001	0.495	0	8.54	1885	1885	0.173	937.3	3730.4	1994.1	263	263	0.75	89.58	11227.5	13075.4	1997	1996	0.251	161.1	876.7	936.8	10	22
51	50	1E-03	0.495	0	8.27	1885	1885	0.175	937.3	3777.8	2018.4	347	343	0.978	107	13322.2	15227	2115	2115	0.269	157.6	862.6	922.96	1	23
59	58	1E-03	0.496	0	7.4	1885	1885	0.175	937.3	3762.3	2008.9	349	349	0.964	102.6	12211.9	14001.1	2126	2125	0.268	168.3	911.2	971.47	2	23
54	54	0.001	0.495	0	8.89	1885	1885	0.176	937.3	3788.6	2019.1	364	350	0.993	117.6	14089.1	15861.8	2099	2098	0.264	142	777.7	837.97	3	23
54	53	9E-04	0.495	0	7.62	1885	1885	0.172	937.3	3717	1995.5	342	342	0.937	103.6	12209	13984.3	2110	2110	0.265	164.5	897.6	957.34	4	23
55	55	0.001	0.495	0	8.3	1885	1885	0.174	937.3	3753.9	2010.3	359	351	0.988	106.6	12711.3	14559	2125	2124	0.268	162.1	883.5	943.8	5	23
49	49	9E-04	0.495	0	7.85	1885	1885	0.176	937.3	3808.1	2044.3	347	345	0.948	97.56	11601.3	13443.2	2124	2123	0.27	167	913	973.77	6	23
51	50	1E-03	0.495	0	8.3	1885	1885	0.174	937.3	3738.9	1988.9	384	355	0.995	119	13897.6	15356.9	2105	2105	0.263	154.5	836.1	895.53	7	23
52	52	8E-04	0.495	0	6.45	1885	1885	0.173	937.3	3750	2010	335	335	0.927	100.2	12063.7	13857.3	2104	2103	0.264	152	821.8	881.74	8	23
48	47	9E-04	0.495	0	8.21	1885	1885	0.176	937.3	3782.1	2023.5	375	352	0.994	121.5	14475.3	15883.8	2091	2091	0.261	141.4	761.6	820.99	9	23
54	53	9E-04	0.495	0	7.74	1885	1885	0.174	937.3	3750.4	2008.5	332	331	0.918	103.4	12443.5	14276	2106	2106	0.263	167.1	904.5	963.83	10	23
63	63	0	0.496	0	0	1885	1885	0.174	937.3	3745.9	2013.4	495	353	0.995	192.7	17043.6	18149	1968	1966	0.25	120.6	664.7	725.81	1	24
51	51	0	0.495	0	0	1885	1885	0.175	937.3	3754.6	2002.2	444	351	0.997	170.7	16930.3	18100.7	1973	1971	0.248	123.8	674.1	734.5	2	24
57	57	0	0.496	0	0	1885	1885	0.176	937.3	3798.7	2031.6	447	355	0.994	176	17408.4	18547.9	1977	1974	0.251	109.9	597.9	659.05	3	24
46	46	0	0.495	0	0	1885	1885	0.175	937.3	3780.8	2006.5	449	352	0.996	174.3	17220.5	18320.5	1984	1982	0.251	120.7	658.6	719.48	4	24
45	45	0	0.495	0	0	1885	1885	0.176	937.3	3805.9	2047.6	493	342	0.996	197.7	17163.7	18234.2	1957	1957	0.245	110.7	597.5	656.94	5	24
56	56	0	0.496	0	0	1885	1885	0.175	937.3	3755.6	2005.4	435	352	0.996	162.4	16403.2	17627.1	2001	1999	0.253	126.9	689.6	750.4	6	24
54	54	0	0.495	0	0	1885	1885	0.175	937.3	3788.5	2014.8	451	351	0.993	183.9	17437.4	18513.6	1959	1958	0.248	106.5	584.8	645.32	7	24
59	59	0	0.496	0	0	1885	1885	0.174	937.3	3742.8	2006.1	470	345	0.995	185.4	17145.4	18224.6	1963	1960	0.249	115.2	636.8	697.98	8	24
45	45	0	0.495	0	0	1885	1885	0.174	937.3	3737.3	1985.1	486	340	0.996	189.3	16964.9	18097.2	1982	1981	0.248	114.8	619.2	679.13	9	24
56	56	0	0.496	0	0	1885	1885	0.174	937.3	3736.9	1985.3	486	356	0.997	196.1	17562.3	18628.1	1965	1964	0.249	105.7	573.6	633.99	10	24
103	102	0.002	0.498	0	8.15	1885	1885	0	0.5	0	0	361	345	1	103.9	13084.4	14867.3	2091	2090	0.261	748.4	4063	2123.2	1	25
103	102	0.002	0.498	0	7.76	1885	1885	0	0.5	0	0	328	327	0.918	91.78	11461.8	13315.8	2095	2095	0.263	762.9	4176	2167	2	25
103	103	0.002	0.498	0	8.6	1885	1885	0	0.5	0	0	339	339	0.915	88.99	10554.7	12303.3	2101	2100	0.265	761.3	4146	2139.1	3	25
103	102	0.002	0.498	0	8.1	1885	1885	0	0.5	0	0	339	338	0.937	97.08	11993.8	13823	2086	2086	0.264	752.7	4110	2164.8	4	25
103	102	0.002	0.498	0	8.4	1885	1885	0	0.5	0	0	382	348	1	119.6	14499.2	16090.9	2088	2088	0.262	738.9	4045	2136.9	5	25
103	102	0.002	0.498	0	8.33	1885	1885	0	0.5	0	0	306	305	0.834	82.89	10081.3	11884.1	2080	2080	0.264	775.1	4262	2215.3	6	25
103	102	0.002	0.498	0	7.76	1885	1885	0	0.5	0	0	331	328	0.893	89.02	10717.1	12562.4	2089	2089	0.262	761.4	4155	2176.6	7	25
103	102	0.002	0.498	0	7.7	1885	1885	0	0.5	0	0	332	331	0.921	100.3	12294.5	14133.6	2073	2073	0.262	752	4139	2183	8	25
103	102	0.002	0.498	0	7.37	1885	1885	0	0.5	0	0	310	309	0.844	86.06	10345.2	12145.8	2084	2084	0.262	767.5	4175	2156.3	9	25

103	102	0.002	0.498	0	7.95	1885	1885	0	0.5	0	0	333	333	0.921	89.39	10936.9	12729.6	2085	2085	0.265	767.4	4248	2203.4	10	25
103	102	0.002	0.498	0	7.78	1885	1885	0	0.5	0	0	464	342	1	203.5	20275.6	21451.3	2005	2005	0.254	654.6	3609	2092.6	1	26
103	102	0.002	0.498	0	7.69	1885	1885	0	0.5	0	0	445	355	1	192	20088.2	21319.5	2017	2017	0.256	655.7	3618	2072.6	2	26
103	102	0.002	0.498	0	8.13	1885	1885	0	0.5	0	0	491	367	1	200.5	19536.9	20793.7	2038	2037	0.258	660.6	3645	2082.9	3	26
103	102	0.002	0.498	0	7.85	1885	1885	0	0.5	0	0	477	339	1	207	20222.9	21394.9	2007	2007	0.254	650.3	3576	2061.9	4	26
103	102	0.002	0.498	0	8.42	1885	1885	0	0.5	0	0	475	360	1	208.6	20194.9	21339.5	2012	2011	0.256	647	3577	2080.6	5	26
103	102	0.002	0.498	0	7.79	1885	1885	0	0.5	0	0	484	348	1	197.3	19386.7	20668	2037	2036	0.256	670.3	3639	2056.7	6	26
103	102	0.002	0.498	0	8.55	1885	1885	0	0.5	0	0	493	356	1	216.2	20442.1	21580.6	2002	2001	0.252	646.8	3564	2077.7	7	26
103	102	0.002	0.498	0	8.44	1885	1885	0	0.5	0	0	478	368	1	200	19704.6	20902.8	2029	2027	0.257	654.3	3595	2045.7	8	26
103	102	0.002	0.498	0	7.97	1885	1885	0	0.5	0	0	487	357	1	214.1	20466.1	21625	1998	1998	0.252	649	3555	2066.9	9	26
103	103	0.002	0.498	0	7.71	1885	1885	0	0.5	0	0	498	362	1	210.5	20000.6	21170.6	2012	2011	0.251	648.8	3531	2050.6	10	26
103	102	0.002	0.498	0	8.26	1885	1885	0	0.5	0	0	390	343	1	167.8	20102.5	21294	1910	1910	0.24	675.9	3667	2162.4	1	27
103	102	0.002	0.498	0	8.51	1885	1885	0	0.5	0	0	387	344	1	171	20814.6	21971	1907	1907	0.241	669.4	3670	2181.9	2	27
103	102	0.002	0.498	0	7.43	1885	1885	0	0.5	0	0	351	347	0.984	150.1	18740.4	20574.5	1942	1942	0.246	680.2	3738	2174.2	3	27
103	102	0.002	0.498	0	8.38	1885	1885	0	0.5	0	0	401	365	1	169.9	20211.8	21422.3	1924	1924	0.246	670.1	3716	2184.3	4	27
103	102	0.002	0.498	0	7.86	1885	1885	0	0.5	0	0	392	355	1	169.1	20615.7	21819.8	1932	1931	0.245	672.8	3692	2184.8	5	27
103	102	0.002	0.498	0	7.72	1885	1885	0	0.5	0	0	403	358	1	178	20250.5	21394.7	1913	1913	0.243	670.2	3700	2169.1	6	27
103	102	0.002	0.498	0	8.14	1885	1885	0	0.5	0	0	378	360	1	161.9	19715.7	21098.2	1928	1928	0.242	675.5	3700	2157.5	7	27
103	102	0.002	0.498	0	8.44	1885	1885	0	0.5	0	0	361	360	0.97	151	18196.3	19981	1957	1957	0.247	685.5	3766	2156.8	8	27
103	102	0.002	0.498	0	7.64	1885	1885	0	0.5	0	0	366	354	0.999	149.4	18696	20790.1	1951	1951	0.245	682.3	3739	2164.6	9	27
103	102	0.002	0.498	0	7.98	1885	1885	0	0.5	0	0	398	352	1	170.7	20169.8	21370.8	1921	1921	0.243	672.8	3710	2182.5	10	27
103	102	0.002	0.498	0	7.72	1885	1885	0	0.5	0	0	241	241	0.675	87.77	11111.7	12927.9	2052	2052	0.239	765	4195	2223.2	1	28
103	102	0.002	0.498	0	8.04	1885	1885	0	0.5	0	0	202	202	0.535	64.28	7670.53	9387.67	2036	2036	0.238	798.3	4384	2260.1	2	28
103	102	0.002	0.498	0	8.39	1885	1885	0	0.5	0	0	221	221	0.634	80.95	10559	12418.6	2035	2035	0.255	773.6	4192	2215.5	3	28
103	102	0.002	0.498	0	8.52	1885	1885	0	0.5	0	0	210	210	0.566	70.77	8715.7	10461.8	2036	2036	0.257	786.6	4323	2277.7	4	28
103	102	0.002	0.498	0	8.22	1885	1885	0	0.5	0	0	231	231	0.619	79.4	9693.79	11430.8	2051	2051	0.239	774.7	4253	2235.9	5	28
103	102	0.002	0.498	0	7.83	1885	1885	0	0.5	0	0	234	234	0.662	84.28	10713.9	12546.2	2039	2039	0.256	767.7	4187	2214.1	6	28
103	102	0.002	0.498	0	8.05	1885	1885	0	0.5	0	0	231	230	0.639	82.49	10269.3	12113.9	2050	2050	0.261	769.2	4267	2262	7	28
103	102	0.002	0.498	0	8.74	1885	1885	0	0.5	0	0	223	223	0.628	79.06	10232.2	12056.7	2047	2047	0.239	776.1	4275	2257.4	8	28
103	102	0.002	0.498	0	7.54	1885	1885	0	0.5	0	0	233	233	0.654	79.52	10242.1	12061.2	2052	2052	0.256	771.1	4200	2230.1	9	28
103	102	0.002	0.498	0	8.34	1885	1885	0	0.5	0	0	226	226	0.637	79.81	10183.9	12010.4	2054	2054	0.258	776.2	4228	2237.6	10	28
103	102	0.002	0.498	0	7.55	1885	1885	0	0.5	0	0	395	356	1	169.2	20264	21505.8	1919	1919	0.242	680.2	3706	2162.8	1	29
103	102	0.002	0.498	0	7.69	1885	1885	0	0.5	0	0	386	349	1	168.5	19917.3	21103.7	1933	1933	0.244	675.9	3701	2160.1	2	29
103	102	0.002	0.498	0	8.15	1885	1885	0	0.5	0	0	435	356	1	196.5	20514.8	21639.4	1910	1909	0.242	664.8	3644	2160.2	3	29
103	103	0.002	0.498	0	8.2	1885	1885	0	0.5	0	0	395	358	1	170	19873.2	21107.3	1948	1948	0.246	672.4	3676	2148.8	4	29
103	102	0.002	0.498	0	8.46	1885	1885	0	0.5	0	0	408	350	1	177.5	20178.3	21414.7	1938	1938	0.243	676.5	3682	2141.3	5	29

103	102	0.002	0.498	0	8.27	1885	1885	0	0.5	0	0	405	352	1	171.8	19823.8	21027.8	1942	1942	0.244	678	3707	2146.6	6	29
103	102	0.002	0.498	0	7.53	1885	1885	0	0.5	0	0	429	356	1	195	20798.1	21915.1	1894	1894	0.24	666.2	3644	2176	7	29
103	102	0.002	0.498	0	8.22	1885	1885	0	0.5	0	0	417	347	1	184.7	20701.3	21871.2	1920	1920	0.243	673	3706	2179.8	8	29
103	102	0.002	0.498	0	7.87	1885	1885	0	0.5	0	0	386	355	1	159.2	19181.5	20499.7	1969	1968	0.249	686.1	3798	2183.3	9	29
103	102	0.002	0.498	0	7.98	1885	1885	0	0.5	0	0	433	355	1	193	20561.7	21717.1	1920	1920	0.243	667.7	3658	2159.2	10	29
103	102	0.002	0.498	0	7.53	1885	1885	0	0.5	0	0	247	247	0.661	84.09	10130	11864.8	2071	2071	0.262	767.4	4220	2222.6	1	30
103	102	0.002	0.498	0	8.56	1885	1885	0	0.5	0	0	260	260	0.709	89.04	10944.9	12712.8	2071	2071	0.261	759.2	4167	2170	2	30
103	102	0.002	0.498	0	9.02	1885	1885	0	0.5	0	0	264	264	0.743	96.39	12264.6	14089.4	2066	2066	0.258	748.3	4060	2153.6	3	30
103	102	0.002	0.498	0	7.97	1885	1885	0	0.5	0	0	255	254	0.718	87.04	10855.8	12725.6	2076	2076	0.263	759.3	4176	2177.5	4	30
103	102	0.002	0.498	0	7.96	1885	1885	0	0.5	0	0	282	281	0.783	91.47	11355.1	13198.7	2096	2096	0.265	750.3	4143	2189.4	5	30
103	102	0.002	0.498	0	8.77	1885	1885	0	0.5	0	0	256	255	0.716	89.05	11184.5	13044.3	2063	2063	0.262	757.5	4185	2226	6	30
103	102	0.002	0.498	0	9.11	1885	1885	0	0.5	0	0	270	270	0.749	94.47	11788.6	13586.4	2084	2084	0.263	746.9	4109	2163.4	7	30
103	102	0.002	0.498	0	8.06	1885	1885	0	0.5	0	0	268	267	0.769	91.11	11601.5	13508.5	2078	2078	0.263	750.2	4128	2183.9	8	30
103	102	0.002	0.498	0	8.64	1885	1885	0	0.5	0	0	268	268	0.738	99.78	12371	14154.6	2051	2051	0.259	741	4056	2176.4	9	30
103	102	0.002	0.498	0	7.61	1885	1885	0	0.5	0	0	253	253	0.688	82.85	10251.3	12014.1	2079	2079	0.263	764.5	4215	2212.6	10	30
103	102	0.002	0.498	0	8.06	1885	1885	0	0.5	0	0	129	129	0.37	41.92	5695.16	7554.65	1960	1960	0.245	821.5	4460	2428.2	1	31
103	102	0.002	0.498	0	8.66	1885	1885	0	0.5	0	0	140	139	0.391	47.51	6397.68	8262.45	1948	1948	0.245	818.7	4479	2424.5	2	31
103	102	0.002	0.498	0	8.61	1885	1885	0	0.5	0	0	120	120	0.339	38.83	5340.53	7170.87	1961	1961	0.247	831.7	4572	2436.3	3	31
103	102	0.002	0.498	0	8.35	1885	1885	0	0.5	0	0	146	146	0.393	54.07	6702.54	8447.26	1948	1948	0.246	806.9	4393	2396.4	4	31
103	102	0.002	0.498	0	8.45	1885	1885	0	0.5	0	0	143	141	0.406	47.45	6545.9	8487.98	1948	1948	0.247	813.9	4510	2454.3	5	31
103	102	0.002	0.498	0	7.65	1885	1885	0	0.5	0	0	144	143	0.411	49.93	6898.42	8801.8	1945	1945	0.244	810	4423	2416.7	6	31
103	102	0.002	0.498	0	7.27	1885	1885	0	0.5	0	0	120	120	0.303	40.42	4999.91	6637.95	1964	1964	0.249	831.9	4588	2441.8	7	31
103	102	0.002	0.498	0	8.42	1885	1885	0	0.5	0	0	164	164	0.458	61.53	8054.53	9865.88	1946	1946	0.246	794.8	4341	2361.1	8	31
103	102	0.002	0.498	0	8.77	1885	1885	0	0.5	0	0	159	159	0.44	60.5	7870.12	9664.68	1946	1946	0.246	795.8	4344	2376.1	9	31
103	102	0.002	0.498	0	8.3	1885	1885	0	0.5	0	0	133	132	0.379	46.17	6556.13	8461.72	1953	1953	0.246	818.9	4463	2394.3	10	31
103	103	0	0.498	0	0	1885	1885	0	0.5	0	0	296	296	0	0.499	0	0	1988	1987	0.252	896.7	4960	2578.2	1	32
103	103	0	0.498	0	0	1885	1885	0	0.5	0	0	318	318	0	0.499	0	0	1988	1987	0.253	896.8	4975	2580.7	2	32
103	103	0	0.498	0	0	1885	1885	0	0.5	0	0	301	301	0	0.499	0	0	1988	1987	0.253	896.7	4960	2559.5	3	32
103	103	0	0.498	0	0	1885	1885	0	0.5	0	0	337	337	0	0.499	0	0	1988	1987	0.251	896.7	4942	2544.9	4	32
103	103	0	0.498	0	0	1885	1885	0	0.5	0	0	285	285	0	0.499	0	0	1988	1987	0.251	896.6	4903	2543.9	5	32
103	103	0	0.498	0	0	1885	1885	0	0.5	0	0	310	310	0	0.499	0	0	1988	1987	0.252	896.7	4964	2575.1	6	32
103	103	0	0.498	0	0	1885	1885	0	0.5	0	0	290	290	0	0.499	0	0	1988	1987	0.254	896.7	4933	2533.1	7	32
103	103	0	0.498	0	0	1885	1885	0	0.5	0	0	330	330	0	0.499	0	0	1988	1987	0.251	896.7	4942	2570.1	8	32
103	103	0	0.498	0	0	1885	1885	0	0.5	0	0	297	297	0	0.499	0	0	1988	1987	0.251	896.6	4922	2539.5	9	32
103	103	0	0.498	0	0	1885	1885	0	0.5	0	0	322	322	0	0.499	0	0	1988	1987	0.252	896.7	4930	2550.1	10	32
82	82	0	0.497	0	0	1885	1885	0	0.5	0	0	370	349	1	132.6	16527.4	18129.7	2032	2031	0.258	723.7	3983	2157.7	1	33

78	78	0	0.497	0	0	1885	1885	0	0.5	0	0	382	346	1	145	17489.5	18941.9	1998	1998	0.252	721.3	3951	2197.5	2	33
80	80	0	0.497	0	0	1885	1885	0	0.5	0	0	376	358	1	124	15152.5	16884.8	2053	2052	0.257	726	3996	2115.7	3	33
78	78	0	0.497	0	0	1885	1885	0	0.5	0	0	403	339	1	147.8	17197.4	18671	1999	1998	0.252	724.1	3985	2190.8	4	33
84	84	0	0.497	0	0	1885	1885	0	0.5	0	0	369	347	1	130.8	16555.8	18100.3	2025	2024	0.256	724.9	4007	2203.9	5	33
79	79	0	0.497	0	0	1885	1885	0	0.5	0	0	417	361	1	152.7	16897.5	18308.9	2016	2015	0.256	710.6	3913	2161.4	6	33
67	67	0	0.496	0	0	1885	1885	0	0.5	0	0	423	345	1	162.8	17927.3	19339.1	1989	1987	0.248	712.3	3874	2148.1	7	33
76	76	0	0.497	0	0	1885	1885	0	0.5	0	0	404	351	1	149.7	17351.4	18823.9	2002	2001	0.251	717.2	3915	2172.9	8	33
77	77	0	0.497	0	0	1885	1885	0	0.5	0	0	434	344	1	169	18567.6	20010.9	1983	1982	0.251	711	3908	2175.4	9	33
73	73	0	0.497	0	0	1885	1885	0	0.5	0	0	449	352	1	172.5	18225.6	19610.2	1985	1984	0.251	700.6	3875	2188.6	10	33
19	19	4E-04	0.487	0	9.13	1885	1885	0	0.5	0	0	316	316	0.895	81.33	10343	12179.2	2084	2083	0.261	778.6	4206	2163	1	34
33	33	6E-04	0.493	0	7.58	1885	1885	0	0.5	0	0	305	304	0.85	79.41	9950.63	11791.8	2082	2081	0.264	782.3	4310	2226.5	2	34
21	21	4E-04	0.488	0	8.41	1885	1885	0	0.5	0	0	324	323	0.903	69.54	8634.28	10471.1	2108	2107	0.265	781.8	4284	2183.5	3	34
31	31	6E-04	0.492	0	8.95	1885	1885	0	0.5	0	0	299	298	0.811	74.18	9046.96	10839.5	2087	2086	0.266	784.2	4330	2244	4	34
20	20	3E-04	0.488	0	6.79	1885	1885	0	0.5	0	0	302	300	0.865	82.97	10554.4	12488.2	2083	2082	0.264	770.5	4241	2200.7	5	34
30	30	5E-04	0.492	0	7.35	1885	1885	0	0.5	0	0	316	316	0.877	85.64	10613.1	12411.4	2065	2064	0.262	774	4283	2254.4	6	34
33	32	6E-04	0.493	0	7.59	1885	1885	0	0.5	0	0	316	316	0.876	86.54	10670	12465.9	2074	2074	0.262	774.1	4280	2212.4	7	34
26	26	5E-04	0.491	0	7.98	1885	1885	0	0.5	0	0	291	290	0.81	69.79	8670.23	10509.7	2091	2091	0.264	791.1	4315	2230.1	8	34
32	32	6E-04	0.492	0	8.01	1885	1885	0	0.5	0	0	291	291	0.813	75.85	9614.49	11424	2065	2064	0.261	789.8	4355	2273.9	9	34
20	19	4E-04	0.488	0	9.21	1885	1885	0	0.5	0	0	281	279	0.755	76.24	9187.31	10999.6	2054	2054	0.259	792.4	4335	2226.3	10	34
23	22	5E-04	0.489	0	9.22	1885	1885	0	0.5	0	0	257	257	0.72	68.6	8703.66	10518.1	2130	2130	0.269	781.1	4265	2164.5	1	35
25	24	5E-04	0.49	0	9.24	1885	1885	0	0.5	0	0	297	296	0.819	69.39	8554	10372.3	2149	2149	0.269	772.8	4204	2117.6	2	35
26	26	6E-04	0.491	0	9.44	1885	1885	0	0.5	0	0	315	314	0.894	83.94	10546	12424.7	2164	2163	0.274	751	4131	2099.7	3	35
33	32	5E-04	0.493	0	7.34	1885	1885	0	0.5	0	0	282	280	0.773	58.41	7205.64	9040.91	2155	2155	0.269	781.2	4234	2119.2	4	35
26	25	5E-04	0.491	0	7.82	1885	1885	0	0.5	0	0	294	294	0.798	70.95	8617.35	10375.8	2169	2169	0.273	767.1	4196	2113.5	5	35
25	25	5E-04	0.49	0	7.85	1885	1885	0	0.5	0	0	269	268	0.749	65.16	8171.49	10008.1	2138	2137	0.268	780.1	4247	2152.9	6	35
30	30	6E-04	0.492	0	8.92	1885	1885	0	0.5	0	0	289	289	0.811	68.81	8589.63	10407	2158	2157	0.273	771.6	4231	2150.6	7	35
27	27	6E-04	0.491	0	9.28	1885	1885	0	0.5	0	0	314	313	0.892	73.37	9298.69	11170.3	2181	2180	0.276	759	4189	2105	8	35
27	27	5E-04	0.491	0	8.4	1885	1885	0	0.5	0	0	284	282	0.796	68.91	8578.88	10457.7	2145	2144	0.269	775.6	4225	2149	9	35
24	24	5E-04	0.49	0	8.17	1885	1885	0	0.5	0	0	299	299	0.836	80.71	10058.5	11869.5	2145	2144	0.268	758	4108	2077.4	10	35
20	20	4E-04	0.488	0	8.54	1885	1885	0	0.5	0	0	180	180	0.432	36.46	4510.72	6258.57	2038	2037	0.259	841.6	4662	2395.8	1	36
30	30	6E-04	0.492	0	9	1885	1885	0	0.5	0	0	180	180	0.447	37.57	4784.42	6596.29	2039	2038	0.258	844.4	4647	2401.1	2	36
18	18	3E-04	0.486	0	7.83	1885	1885	0	0.5	0	0	147	147	0.406	36.11	4570.33	6358.63	2031	2030	0.255	844.8	4627	2386.1	3	36
22	22	4E-04	0.489	0	8.05	1885	1885	0	0.5	0	0	142	140	0.379	33.7	4163.84	5962.95	2013	2012	0.252	848.5	4605	2403	4	36
24	23	4E-04	0.49	0	7.4	1885	1885	0	0.5	0	0	178	178	0.482	47.54	6058.37	7811.26	2019	2019	0.257	830.1	4594	2381.9	5	36
28	28	5E-04	0.491	0	7.57	1885	1885	0	0.5	0	0	162	161	0.447	46.74	5931.89	7752.51	2024	2023	0.255	828.3	4536	2396.4	6	36
25	25	5E-04	0.49	0	9.05	1885	1885	0	0.5	0	0	186	185	0.495	50.97	6329.57	8096.55	2016	2015	0.254	825.4	4531	2370.6	7	36

25	25	5E-04	0.49	0	8.88	1885	1885	0	0.5	0	0	173	172	0.481	41.12	5297.58	7129.95	2039	2038	0.255	836.4	4536	2332.3	8	36
24	24	4E-04	0.49	0	7.95	1885	1885	0	0.5	0	0	167	166	0.457	41.43	5188.47	6997.91	2033	2032	0.257	838.1	4592	2372.4	9	36
24	24	5E-04	0.49	0	9.82	1885	1885	0	0.5	0	0	169	169	0.482	48.3	6361.85	8211.75	2020	2019	0.253	828.9	4505	2358.3	10	36
26	26	5E-04	0.491	0	8.4	1885	1885	0	0.5	0	0	207	207	0.571	70.03	8762.11	10548.2	2047	2046	0.256	786	4268	2270.3	1	37
23	23	4E-04	0.489	0	7.3	1885	1885	0	0.5	0	0	218	218	0.614	71.23	9031.44	10855.2	2065	2064	0.259	786.7	4288	2227.9	2	37
21	21	4E-04	0.488	0	7.44	1885	1885	0	0.5	0	0	226	226	0.625	79.4	9761.63	11552.7	2049	2048	0.261	771.9	4274	2257.4	3	37
29	29	6E-04	0.492	0	8.29	1885	1885	0	0.5	0	0	223	222	0.62	74.72	9371.3	11220.1	2057	2056	0.259	777.2	4242	2243.3	4	37
31	31	6E-04	0.492	0	7.8	1885	1885	0	0.5	0	0	231	230	0.646	76.31	9778.56	11637.3	2065	2064	0.261	775	4254	2225.4	5	37
27	27	5E-04	0.491	0	8.3	1885	1885	0	0.5	0	0	222	222	0.622	75.37	9765.33	11579.8	2057	2056	0.256	774.8	4217	2232.2	6	37
22	22	6E-04	0.489	0	11.9	1885	1885	0	0.5	0	0	234	233	0.67	80.23	10419.2	12318.6	2070	2069	0.262	772.2	4232	2188.6	7	37
25	24	4E-04	0.49	0	6.72	1885	1885	0	0.5	0	0	242	242	0.667	85.96	10738.6	12524.7	2060	2060	0.26	763.9	4207	2215.8	8	37
29	28	6E-04	0.492	0	9.29	1885	1885	0	0.5	0	0	222	222	0.617	77.92	9783.91	11585.5	2060	2060	0.258	775	4191	2201.4	9	37
23	23	4E-04	0.489	0	7.56	1885	1885	0	0.5	0	0	224	223	0.586	74.89	8878.09	10622	2066	2066	0.262	781.4	4308	2241.2	10	37
28	28	5E-04	0.491	0	7.65	1885	1885	0	0.5	0	0	340	340	0.935	133.4	16319.9	18102.8	2005	2004	0.253	707.1	3864	2157.2	1	38
30	29	5E-04	0.492	0	8.14	1885	1885	0	0.5	0	0	342	342	0.955	131.1	16159.4	17968	2017	2017	0.255	715.2	3958	2186.4	2	38
24	24	5E-04	0.49	0	9.2	1885	1885	0	0.5	0	0	297	296	0.862	107.3	14009.3	15940.8	2016	2015	0.253	745.9	4067	2188.3	3	38
30	30	7E-04	0.492	0	9.86	1885	1885	0	0.5	0	0	328	328	0.89	121.1	14413.1	16170.8	2009	2008	0.254	726.9	3986	2198.2	4	38
21	21	4E-04	0.488	0	9.11	1885	1885	0	0.5	0	0	319	319	0.88	126.6	15684.3	17472	1989	1988	0.251	719.6	3958	2201.3	5	38
29	28	5E-04	0.492	0	7.95	1885	1885	0	0.5	0	0	294	294	0.821	114.4	14442	16251.1	2011	2011	0.255	732.6	4022	2193.3	6	38
30	30	7E-04	0.492	0	9.55	1885	1885	0	0.5	0	0	321	321	0.89	120.6	14972	16768.1	2018	2017	0.254	724.7	3993	2175.5	7	38
25	25	4E-04	0.49	0	6.39	1885	1885	0	0.5	0	0	301	300	0.856	111.9	14107.3	16001.2	2009	2008	0.252	739.3	4037	2199.4	8	38
21	21	4E-04	0.488	0	9.09	1885	1885	0	0.5	0	0	326	326	0.918	124.3	15579.9	17403.8	2044	2043	0.261	720.2	3982	2153.5	9	38
24	24	3E-04	0.49	0	4.84	1885	1885	0	0.5	0	0	294	293	0.834	107.3	13614.6	15503.1	2011	2010	0.254	741.8	4077	2217.2	10	38
27	27	4E-04	0.491	0	7.03	1885	1885	0	0.5	0	0	340	340	0.956	132.9	16636.1	18458.3	2091	2090	0.263	692.4	3824	2081	1	39
25	24	5E-04	0.49	0	9.59	1885	1885	0	0.5	0	0	330	330	0.9	128.2	15531.5	17298.1	2084	2084	0.264	697.1	3889	2116	2	39
22	22	4E-04	0.489	0	7.68	1885	1885	0	0.5	0	0	344	342	0.974	137.1	17491.3	19433.3	2085	2084	0.263	683	3749	2046.2	3	39
19	19	4E-04	0.487	0	9.14	1885	1885	0	0.5	0	0	332	331	0.917	131.6	16284.3	18127.9	2067	2066	0.261	690.2	3810	2105.3	4	39
17	16	3E-04	0.486	0	7.19	1885	1885	0	0.5	0	0	336	335	0.953	135.2	17098	18991.8	2076	2076	0.261	683.9	3749	2067.9	5	39
21	21	5E-04	0.488	0	9.88	1885	1885	0	0.5	0	0	330	328	0.908	132	16319.7	18209.6	2072	2072	0.261	687.9	3744	2053.6	6	39
23	23	4E-04	0.489	0	8.35	1885	1885	0	0.5	0	0	355	354	0.962	136.3	16316.2	18122.7	2091	2089	0.261	681.7	3701	2032.1	7	39
22	22	5E-04	0.489	0	10.3	1885	1885	0	0.5	0	0	379	358	1	152.2	18622.8	20275.8	2070	2069	0.261	664.9	3661	2052	8	39
39	39	7E-04	0.494	0	8.17	1885	1885	0	0.5	0	0	337	337	0.917	131.3	16008.6	17772.5	2087	2086	0.262	688.3	3761	2056	9	39
24	23	5E-04	0.49	0	8.76	1885	1885	0	0.5	0	0	385	357	1	159	19282.7	20593.9	2064	2064	0.259	663	3610	2014.7	10	39
36	36	7E-04	0.493	0	8.18	1885	1885	0	0.5	0	0	233	233	0.666	90.67	11945.4	13796.3	1926	1925	0.244	742.4	4079	2295.6	1	40
21	21	5E-04	0.488	0	9.27	1885	1885	0	0.5	0	0	232	231	0.667	92.27	12036.8	13949	1911	1910	0.239	745.1	4044	2291.9	2	40
19	18	3E-04	0.487	0	7.82	1885	1885	0	0.5	0	0	227	227	0.623	94.7	12186.5	13964.6	1921	1921	0.243	746.9	4120	2326.9	3	40

27	27	6E-04	0.491	0	9.29	1885	1885	0	0.5	0	0	263	239	0.737	102.9	13328.6	15368.3	1903	1903	0.24	725.2	3967	2282	4	40
27	27	5E-04	0.491	0	7.91	1885	1885	0	0.5	0	0	223	222	0.631	90.95	11965.5	13854.8	1923	1922	0.244	744.8	4101	2327.1	5	40
29	29	5E-04	0.492	0	7.15	1885	1885	0	0.5	0	0	240	240	0.632	98.27	12036.2	13743.7	1909	1908	0.243	740.5	4113	2369.8	6	40
21	21	4E-04	0.488	0	8.3	1885	1885	0	0.5	0	0	248	246	0.692	98.02	12635.3	14547.2	1915	1914	0.244	735.5	4064	2325.2	7	40
17	17	3E-04	0.486	0	7.55	1885	1885	0	0.5	0	0	264	264	0.748	107.4	14176.6	16013.8	1923	1922	0.243	710.1	3903	2253.1	8	40
28	27	6E-04	0.491	0	9.11	1885	1885	0	0.5	0	0	226	225	0.656	92.79	12587.2	14527.9	1930	1930	0.246	742.4	4102	2315.1	9	40
19	19	3E-04	0.487	0	7.39	1885	1885	0	0.5	0	0	237	237	0.663	94.61	12060.3	13874.2	1932	1931	0.247	738.1	4091	2313.7	10	40
28	28	5E-04	0.491	0	7.97	1885	1885	0	0.5	0	0	224	224	0.622	84.08	10766.5	12564.9	1972	1971	0.249	741.9	4085	2279.3	1	41
25	25	6E-04	0.49	0	10.3	1885	1885	0	0.5	0	0	222	222	0.589	86.31	10716.3	12436.3	1968	1967	0.251	741.1	4081	2255	2	41
23	23	4E-04	0.489	0	7.06	1885	1885	0	0.5	0	0	239	237	0.64	96.68	11954.1	13791.3	1966	1965	0.25	725.1	3995	2249.2	3	41
29	28	5E-04	0.492	0	8.47	1885	1885	0	0.5	0	0	240	239	0.668	93.86	11910.3	13764.5	1963	1963	0.249	731.7	4037	2270.4	4	41
19	19	3E-04	0.487	0	6.72	1885	1885	0	0.5	0	0	193	192	0.523	72.41	9133.33	10946	1965	1965	0.246	768.9	4199	2294.9	5	41
28	28	5E-04	0.491	0	7.45	1885	1885	0	0.5	0	0	208	208	0.563	83.49	10567.6	12322.4	1971	1970	0.249	745.7	4106	2283.1	6	41
26	26	5E-04	0.491	0	8.83	1885	1885	0	0.5	0	0	206	206	0.564	77.67	9846.54	11621	1969	1968	0.247	754.5	4088	2274.9	7	41
27	27	5E-04	0.491	0	7.46	1885	1885	0	0.5	0	0	232	231	0.644	93.37	12066.8	13924.1	1967	1966	0.249	729.1	4038	2301	8	41
33	33	7E-04	0.493	0	9.06	1885	1885	0	0.5	0	0	198	198	0.549	73.34	9475.24	11273.5	1971	1970	0.247	760.1	4170	2317.2	9	41
19	19	3E-04	0.487	0	6.94	1885	1885	0	0.5	0	0	221	220	0.632	87.04	11231.2	13134.7	1961	1960	0.247	743.9	4080	2266.9	10	41
103	102	0.002	0.498	0	7.91	1885	1885	0.173	937.3	3728.6	1963.7	197	197	0.561	51.58	6518.86	8363.75	1959	1959	0.25	185.6	1023	1083.5	1	42
103	102	0.002	0.498	0	7.89	1885	1885	0.177	937.3	3803.7	2031.2	192	192	0.535	46.31	5542.13	7349.04	1966	1966	0.249	173	948.2	1008.5	2	42
103	102	0.002	0.498	0	7.56	1885	1885	0.175	937.3	3775.7	2019.5	197	197	0.536	51.74	6154.68	7916.89	1964	1963	0.247	158.5	866.6	926.88	3	42
103	102	0.002	0.498	0	7.93	1885	1885	0.174	937.3	3743.9	1999	202	201	0.555	57.11	6922.57	8743.21	1961	1961	0.249	174.2	956.2	1016.5	4	42
103	102	0.002	0.498	0	7.59	1885	1885	0.176	937.3	3811.8	2053.8	193	192	0.518	48.65	5705.21	7481.41	1964	1964	0.249	176.5	955.7	1015.9	5	42
103	102	0.002	0.498	0	8.69	1885	1885	0.174	937.3	3767.2	2019.1	167	167	0.479	39.69	5046.96	6904.3	1963	1963	0.249	190.1	1047	1107	6	42
103	102	0.002	0.498	0	7.31	1885	1885	0.174	937.3	3736.1	1988.7	195	195	0.562	50.48	6200.34	8068.16	1950	1950	0.245	167.5	907.5	967.11	7	42
103	102	0.002	0.498	0	8.01	1885	1885	0.174	937.3	3755.3	2003.3	192	192	0.513	49.92	5896.64	7627.91	1963	1963	0.248	175	956.9	1017	8	42
103	102	0.002	0.498	0	7.86	1885	1885	0.175	937.3	3779.1	2021.5	162	162	0.46	38.1	4592.75	6431.22	1962	1962	0.249	180.8	989.3	1049.6	9	42
103	102	0.002	0.498	0	8.42	1885	1885	0.174	937.3	3750.2	2004.3	175	175	0.48	43.42	5161.48	6940.02	1964	1964	0.248	188.1	1026	1085.9	10	42
103	102	0.002	0.498	0	7.39	1885	1885	0.175	937.3	3759.7	2006.4	126	124	0.34	22.9	2704.1	4512.47	1956	1956	0.247	204.6	1123	1182.7	1	43
103	102	0.002	0.498	0	8.3	1885	1885	0.174	937.3	3768.7	2021.7	99	98	0.28	10.28	1280.1	3118.28	1957	1957	0.247	216.3	1181	1241.2	2	43
103	102	0.002	0.498	0	8.81	1885	1885	0.176	937.3	3809.4	2049.2	99	99	0.29	9.894	1350.38	3250.89	1963	1963	0.25	213.6	1177	1237.2	3	43
103	102	0.002	0.498	0	8.57	1885	1885	0.175	937.3	3759.6	2008.4	113	113	0.322	19.44	2435.01	4283.84	1960	1960	0.248	205.5	1122	1182.1	4	43
103	102	0.002	0.498	0	7.7	1885	1885	0.173	937.3	3739.2	2007.5	92	90	0.253	9.73	1131.78	2955.9	1955	1955	0.247	221.4	1213	1273	5	43
103	102	0.002	0.498	0	7.95	1885	1885	0.175	937.3	3776.4	2025.8	108	107	0.298	18.5	2228.49	4043.89	1951	1951	0.245	205.6	1118	1177.4	6	43
103	102	0.002	0.498	0	7.94	1885	1885	0.175	937.3	3768	1999.2	106	106	0.281	16.67	1900.74	3620.21	1962	1962	0.25	218.3	1194	1254.5	7	43
103	102	0.002	0.498	0	8.59	1885	1885	0.174	937.3	3755.2	2014.3	109	108	0.295	14.79	1753.98	3535.02	1964	1964	0.247	211.7	1148	1207.8	8	43
103	102	0.002	0.498	0	7.72	1885	1885	0.176	937.3	3801.7	2034.1	98	97	0.26	8.02	984.94	2710.98	1965	1965	0.247	210.6	1141	1201.1	9	43

103	102	0.002	0.498	0	8.3	1885	1885	0.174	937.3	3742	2001.4	109	108	0.312	15.95	1967.23	3851.54	1955	1955	0.248	220.5	1201	1261.6	10	43
103	102	0.002	0.498	0	8.87	1885	1885	0.172	937.3	3703.1	1984	205	205	0.601	49.54	6408.63	8308.35	2090	2090	0.263	219.9	1200	1259.5	1	44
103	102	0.002	0.498	0	8.86	1885	1885	0.176	937.3	3782.8	2030.4	171	171	0.48	34.98	4177.78	5998.19	2056	2056	0.258	219.5	1185	1244.1	2	44
103	102	0.002	0.498	0	8.38	1885	1885	0.174	937.3	3746.9	2002.9	198	198	0.544	47.41	5711.28	7491.68	2080	2080	0.263	226.5	1237	1297.3	3	44
103	102	0.002	0.498	0	8.38	1885	1885	0.174	937.3	3745.6	2001.4	203	202	0.56	48.41	5645.27	7456.15	2077	2077	0.261	206.8	1131	1190.2	4	44
103	102	0.002	0.498	0	7.97	1885	1885	0.176	937.3	3781.7	2016.5	200	198	0.55	44.24	5256.07	7091.3	2087	2087	0.264	214.7	1172	1231.8	5	44
103	102	0.002	0.498	0	8.16	1885	1885	0.174	937.3	3750.1	2003.7	180	180	0.518	40.14	4995.41	6861.86	2060	2060	0.26	220.6	1201	1261.2	6	44
103	102	0.002	0.498	0	8.45	1885	1885	0.174	937.3	3767.8	2027.5	182	182	0.486	40.93	4656.75	6386.14	2071	2071	0.262	218.6	1200	1259.7	7	44
103	102	0.002	0.498	0	7.91	1885	1885	0.172	937.3	3715.7	1990.3	196	195	0.567	42.44	5420.13	7324.92	2079	2079	0.262	226.2	1228	1287.5	8	44
103	102	0.002	0.498	0	7.79	1885	1885	0.175	937.3	3775.3	2022.1	196	195	0.562	43.5	5479.14	7367.77	2074	2074	0.262	211.7	1155	1215.3	9	44
103	102	0.002	0.498	0	8.21	1885	1885	0.174	937.3	3780.3	2021.2	184	183	0.543	45.26	5954.62	7899.54	2062	2062	0.26	209.7	1143	1202.5	10	44
103	103	0.002	0.498	0	8.64	1885	1885	0.176	937.3	3797.1	2032.1	296	296	0.817	97.7	11632.4	13421	2027	2026	0.256	153.9	837.7	898.02	1	45
103	102	0.002	0.498	0	7.53	1885	1885	0.174	937.3	3730.1	1981.7	301	299	0.813	95.02	11170.9	13002.9	2041	2041	0.26	168.3	925	985.46	2	45
103	103	0.002	0.498	0	8.73	1885	1885	0.176	937.3	3785.2	2038.4	288	287	0.779	92.09	10633.8	12426.2	2014	2013	0.254	163	893.7	954.19	3	45
103	102	0.002	0.498	0	8.31	1885	1885	0.174	937.3	3772.9	2028.5	305	304	0.843	96.38	11608.7	13438.5	2011	2011	0.254	162.1	874.6	934.58	4	45
103	102	0.002	0.498	0	7.95	1885	1885	0.174	937.3	3738.8	1999.9	278	278	0.79	92.93	11263.1	13105	2011	2011	0.252	155.2	839.9	899.41	5	45
103	102	0.002	0.498	0	7.4	1885	1885	0.174	937.3	3751.9	2015.9	288	288	0.797	89.84	10807.6	12800.7	2033	2033	0.255	166.6	901.1	980.66	6	45
103	102	0.002	0.498	0	8.19	1885	1885	0.176	937.3	3788.4	2024.7	287	287	0.771	90.3	10485.9	12227.9	2043	2043	0.258	162	887.6	947.62	7	45
103	102	0.002	0.498	0	8.21	1885	1885	0.177	937.3	3807.7	2032.7	296	295	0.806	92.22	10775.7	12578.5	2035	2035	0.255	144	785.4	845	8	45
103	102	0.002	0.498	0	7.54	1885	1885	0.174	937.3	3765.4	2037.5	292	291	0.809	94.23	11235.6	13073.6	2020	2020	0.255	165.4	896.1	956.09	9	45
103	102	0.002	0.498	0	8.37	1885	1885	0.176	937.3	3784.1	2019	301	301	0.824	95.63	11351.2	13124.9	2020	2020	0.257	162.1	890.2	950.52	10	45
103	102	0.002	0.498	0	7.52	1885	1885	0.173	937.3	3702	1989.7	311	310	0.825	108.5	12503.7	14266.3	2046	2046	0.256	145.2	787.3	846.69	1	46
103	102	0.002	0.498	0	8	1885	1885	0.174	937.3	3753	2002.7	319	319	0.892	108.9	13223.6	15036.2	2038	2037	0.258	138.1	752.9	813.4	2	46
103	102	0.002	0.498	0	7.96	1885	1885	0.174	937.3	3743.5	1996.9	305	305	0.841	101.7	12294.2	14081.6	2025	2025	0.256	148.3	809.7	869.69	3	46
103	102	0.002	0.498	0	8.01	1885	1885	0.174	937.3	3761.6	2003.9	306	306	0.844	104.8	12681.5	14468.6	2039	2039	0.26	150.7	825.9	886.35	4	46
103	102	0.002	0.498	0	7.9	1885	1885	0.175	937.3	3779.9	2025.3	310	309	0.863	105.1	12761.7	14610.6	2044	2044	0.257	143.9	777.3	837.14	5	46
103	102	0.002	0.498	0	8.18	1885	1885	0.174	937.3	3744.1	1980.7	300	298	0.827	99.56	12061.2	13933.2	2024	2024	0.257	157.7	863.9	924.22	6	46
103	102	0.002	0.498	0	8.46	1885	1885	0.174	937.3	3757.9	2028.6	310	308	0.872	106	13075.5	14988.3	2020	2020	0.254	148.5	803.7	863.47	7	46
103	102	0.002	0.498	0	8.16	1885	1885	0.172	937.3	3688.5	1957.4	336	333	0.928	116.7	13932.9	15851.8	2030	2030	0.257	146	796.8	856.92	8	46
103	102	0.002	0.498	0	8.04	1885	1885	0.173	937.3	3721.7	1986.7	306	305	0.844	105.5	12431.5	14260.1	2043	2043	0.259	158.4	865.6	925.74	9	46
103	102	0.002	0.498	0	8.19	1885	1885	0.174	937.3	3733.9	1989.1	302	299	0.813	102	12066.2	13940.5	2035	2035	0.256	146	798.7	858.43	10	46
103	103	0.002	0.498	0	8.39	1885	1885	0.176	937.3	3810.6	2030.3	354	353	0.968	125.2	14699.3	16471.4	1990	1989	0.25	116.6	639.3	699.42	1	47
103	102	0.002	0.498	0	7.89	1885	1885	0.175	937.3	3770.8	2024.9	370	341	0.993	138.7	17150.6	18418.5	1958	1958	0.247	112.9	617.3	677.16	2	47
103	102	0.002	0.498	0	7.92	1885	1885	0.174	937.3	3764.2	2014.9	350	347	0.963	123.5	14898.7	16809.6	1964	1964	0.248	120.5	655.9	715.93	3	47
103	103	0.002	0.498	0	7.9	1885	1885	0.174	937.3	3752	2000.1	356	353	0.976	126.3	15131.8	17010.7	1980	1979	0.249	117.4	641.4	701.6	4	47
103	102	0.002	0.498	0	7.98	1885	1885	0.176	937.3	3788.1	2015.6	366	356	0.992	128.4	15359.3	17386.4	1992	1991	0.251	121.4	665.4	725.7	5	47

103	102	0.002	0.498	0	7.96	1885	1885	0.175	937.3	3763.1	2018.5	365	349	0.995	137.4	16535.2	18135.1	1967	1966	0.248	114.5	623.6	683.87	6	47
103	102	0.002	0.498	0	7.8	1885	1885	0.173	937.3	3713.5	1982.8	358	357	0.967	129.3	15109	16877.6	1979	1979	0.248	124.3	676.6	736.23	7	47
103	102	0.002	0.498	0	7.51	1885	1885	0.172	937.3	3692.8	1965.1	325	325	0.857	113.7	13091.3	14800.9	2002	2002	0.254	147.5	809.4	869.62	8	47
103	102	0.002	0.498	0	8.27	1885	1885	0.176	937.3	3799.5	2033	344	341	0.968	118.3	14716.6	16654.9	1970	1970	0.249	117	640.1	700.1	9	47
103	102	0.002	0.498	0	7.99	1885	1885	0.173	937.3	3720	1987	350	349	0.963	122.3	14466.6	16294.2	1984	1984	0.251	126.8	689	749.06	10	47
103	102	0.002	0.498	0	7.36	1885	1885	0.175	937.3	3772.9	2013.7	444	354	0.996	169.2	16393.7	17770.9	2022	2022	0.256	114	627.5	687.69	1	48
103	102	0.002	0.498	0	8.04	1885	1885	0.174	937.3	3740.3	1997.5	455	352	0.997	173.2	16661.7	17794.2	1998	1998	0.252	117.6	635.3	695.17	2	48
103	102	0.002	0.498	0	8.3	1885	1885	0.175	937.3	3778.2	2031	445	343	0.996	170.5	17076.9	18292.1	2009	2008	0.254	122.8	680.9	741.48	3	48
103	102	0.002	0.498	0	8.32	1885	1885	0.175	937.3	3742.6	1992.1	409	352	0.995	144.9	15665.2	16929.8	2048	2047	0.257	136.4	735.7	795.54	4	48
103	102	0.002	0.498	0	8.36	1885	1885	0.174	937.3	3762.2	2015.5	445	356	0.996	167	16681	17874.5	2024	2023	0.258	132.8	728.7	789.64	5	48
103	102	0.002	0.498	0	8.38	1885	1885	0.176	937.3	3797.8	2033.7	466	344	0.996	181	17071.4	18217.8	2003	2003	0.253	114.6	632.2	692.26	6	48
103	102	0.002	0.498	0	8.61	1885	1885	0.172	937.3	3725.7	1983.1	436	357	0.995	159.7	16340.7	17604.7	2034	2034	0.257	128.6	704.8	764.82	7	48
103	102	0.002	0.498	0	8.17	1885	1885	0.175	937.3	3757.2	2004.9	440	345	0.994	166	16546.9	17778.6	2026	2025	0.257	137.3	751.5	812.15	8	48
103	102	0.002	0.498	0	7.58	1885	1885	0.175	937.3	3781.5	2031.9	475	351	0.997	187.5	17260.9	18333	1989	1988	0.249	102	548.7	608.33	9	48
103	102	0.002	0.498	0	8.63	1885	1885	0.173	937.3	3736.2	1996.1	441	351	0.994	164	16664.8	17909.9	2018	2018	0.257	135.1	746.5	806.94	10	48
103	102	0.002	0.498	0	8.05	1885	1885	0.173	937.3	3726.4	1994.9	392	350	0.992	131.4	15065.7	16456.2	2028	2028	0.256	156.8	851.9	911.79	1	49
103	102	0.002	0.498	0	7.59	1885	1885	0.175	937.3	3762.5	2003.7	392	361	0.995	127.1	14673.4	16078	2036	2036	0.256	146.6	797.5	857.29	2	49
103	102	0.002	0.498	0	7.98	1885	1885	0.175	937.3	3773.5	2012.7	384	358	0.994	126.8	14819	16218.7	2013	2013	0.253	133.1	719.9	779.49	3	49
103	102	0.002	0.498	0	9.24	1885	1885	0.173	937.3	3731.1	1989.4	404	345	0.994	135.9	14819	16230.1	2027	2026	0.255	152.1	828.1	888.36	4	49
103	102	0.002	0.498	0	8.2	1885	1885	0.174	937.3	3766.1	2012.4	391	346	0.996	134	15542	16947.4	2023	2023	0.254	134.2	730.3	789.98	5	49
103	102	0.002	0.498	0	7.97	1885	1885	0.176	937.3	3796.5	2023.4	426	359	0.995	151.2	15621.4	16940.9	2018	2018	0.256	137	747.9	808.14	6	49
103	102	0.002	0.498	0	6.81	1885	1885	0.174	937.3	3746	1997.2	374	355	0.994	116.1	13930	15570.4	2047	2046	0.258	159.9	865.4	925.78	7	49
103	102	0.002	0.498	0	7.72	1885	1885	0.177	937.3	3805.9	2040.5	405	352	0.996	131.1	14762.3	16181.8	1998	1998	0.253	139.4	760.3	820.32	8	49
103	102	0.002	0.498	0	8.1	1885	1885	0.174	937.3	3753.3	2014.7	418	356	0.992	141.8	15467	16787	1997	1997	0.253	139.7	769.4	829.65	9	49
103	102	0.002	0.498	0	7.86	1885	1885	0.174	937.3	3780.6	2008.5	397	353	0.994	128.7	14468	15860.1	2010	2009	0.254	155.7	858.9	919.48	10	49
82	82	0.001	0.497	0	7.88	1885	1885	0.176	937.3	3782.9	2018.4	487	345	0.996	210.9	17946.8	19009.7	1884	1883	0.238	79.44	432.4	492.57	1	50
82	82	0.002	0.497	0	8.32	1885	1885	0.174	937.3	3730.4	1984.6	502	348	0.997	210.2	17486.6	18529.7	1907	1906	0.238	93.77	502.6	562.18	2	50
82	81	0.002	0.497	0	8.35	1885	1885	0.173	937.3	3725.1	1993.7	513	355	0.997	219.3	17554	18566.7	1897	1896	0.241	87.79	479.6	540.26	3	50
90	89	0.002	0.497	0	8.77	1885	1885	0.174	937.3	3744.6	1991.1	534	342	0.996	233.5	18219.4	19296.9	1868	1868	0.234	88.45	475.4	534.93	4	50
81	80	0.002	0.497	0	8.15	1885	1885	0.175	937.3	3773.8	2017	511	354	0.997	214.8	17581.8	18613.1	1884	1883	0.236	85.34	463.5	523.27	5	50
80	80	0.002	0.497	0	8.96	1885	1885	0.175	937.3	3765.9	2011.4	516	361	0.994	218.3	17661.1	18675.3	1890	1889	0.239	87.9	478.7	538.99	6	50
74	73	0.001	0.497	0	8.43	1885	1885	0.173	937.3	3751	2017.8	512	349	0.996	219.5	17726.5	18753.5	1879	1878	0.237	83.11	452.5	512.69	7	50
80	80	0.002	0.497	0	8.69	1885	1885	0.175	937.3	3789.8	2040.7	530	360	0.997	223.5	17490.6	18489.6	1868	1867	0.239	84.52	469.9	531.03	8	50
88	87	0.002	0.497	0	9.31	1885	1885	0.175	937.3	3800.4	2049.5	527	348	0.995	227.8	17843.4	18879.1	1886	1884	0.238	77.56	426.3	486.89	9	50
83	82	0.001	0.497	0	7.88	1885	1885	0.175	937.3	3772.1	2016	477	355	0.995	198.5	17539	18572	1901	1899	0.241	98.12	537.5	598.52	10	50
80	79	0.001	0.497	0	7.76	1885	1885	0.174	937.3	3766	2019.7	426	360	0.996	152	15797	17103.4	2067	2065	0.258	129	698.8	758.86	1	51

82	81	0.002	0.497	0	8.41	1885	1885	0.173	937.3	3725.9	2004.1	392	365	0.996	137.3	15583.9	16960.3	2085	2085	0.263	141.9	767.5	827.44	2	51
81	80	0.002	0.497	0	8.42	1885	1885	0.175	937.3	3742.3	1997.4	402	364	0.995	135	15341.1	16700.6	2088	2088	0.263	134.8	738.8	798.67	3	51
70	69	0.001	0.496	0	8.1	1885	1885	0.173	937.3	3734.5	1999.4	415	363	0.995	153.5	16315.4	17557.5	2053	2053	0.26	132.5	722.9	783.01	4	51
75	74	0.001	0.497	0	8.49	1885	1885	0.174	937.3	3738.9	1998.7	429	349	0.997	166	17068.9	18250.6	2024	2024	0.256	123.8	671.3	731.37	5	51
84	83	0.001	0.497	0	7.69	1885	1885	0.175	937.3	3755.4	2000.4	401	349	0.995	145.7	16254.5	17509.9	2047	2047	0.257	128.8	697.8	757.39	6	51
75	74	0.001	0.497	0	8.05	1885	1885	0.174	937.3	3748.3	1988.1	404	359	0.996	140.6	15419	16725.7	2068	2068	0.261	132.8	725.9	785.87	7	51
78	77	0.001	0.497	0	8.2	1885	1885	0.175	937.3	3759.3	1999.8	407	346	0.995	144.4	15999.5	17344.4	2057	2056	0.259	142.1	773.8	834.08	8	51
77	76	0.001	0.497	0	7.83	1885	1885	0.176	937.3	3780.1	2007.2	413	359	0.996	140.7	15479.1	16848.5	2073	2072	0.263	135.4	741.6	802.34	9	51
76	75	0.001	0.497	0	8.14	1885	1885	0.175	937.3	3750.1	1997.8	425	349	0.995	156.4	16351.8	17639.9	2053	2052	0.258	134.1	722.1	782.21	10	51
83	82	0.002	0.497	0	8.38	1885	1885	0.175	937.3	3778.3	2019.7	290	290	0.79	90.64	10789.6	12554.8	2002	2002	0.25	150.5	814.3	873.66	1	52
74	73	0.001	0.497	0	8.65	1885	1885	0.173	937.3	3741.8	2015.6	303	302	0.825	106.4	12630.5	14441.8	1987	1987	0.251	137.9	751.9	811.8	2	52
78	77	0.002	0.497	0	8.48	1885	1885	0.175	937.3	3747.2	1997.3	304	303	0.876	101.4	12593.5	14506.1	1998	1998	0.254	159.1	872.6	933.02	3	52
72	72	0.001	0.497	0	7.7	1885	1885	0.174	937.3	3748.9	2002.6	318	317	0.901	111.7	13601.6	15485.6	1997	1996	0.253	140.4	770.8	831.35	4	52
77	77	0.001	0.497	0	8.16	1885	1885	0.177	937.3	3803.3	2033.1	313	311	0.825	104.7	12270.2	14065.4	1995	1995	0.252	135.4	741.7	801.69	5	52
83	82	0.002	0.497	0	8.25	1885	1885	0.176	937.3	3773.6	2008.3	298	297	0.804	97.58	11500.5	13291.1	1996	1996	0.252	134.8	740.9	800.91	6	52
79	78	0.001	0.497	0	6.92	1885	1885	0.174	937.3	3746	2021.9	333	331	0.921	120	14154.6	16031.4	1983	1983	0.25	133.2	728.7	788.59	7	52
82	81	0.002	0.497	0	8.26	1885	1885	0.175	937.3	3787	2018.1	294	294	0.804	100.3	11884.7	13657.8	1994	1994	0.255	141.3	782.4	843.19	8	52
74	73	0.001	0.497	0	8.1	1885	1885	0.173	937.3	3742.6	2008.1	286	285	0.814	92.86	11330.1	13219.9	1985	1985	0.251	153.7	841.1	901.17	9	52
78	77	0.001	0.497	0	7.89	1885	1885	0.175	937.3	3736.3	1993.2	307	307	0.852	107.7	13204.9	15004	1970	1970	0.248	136.3	736.8	796.55	10	52
73	72	0.001	0.497	0	7.48	1885	1885	0.173	937.3	3710.2	1976.8	427	355	0.997	172.5	17377.3	18402.4	1958	1958	0.248	107.5	585.8	645.93	1	53
81	80	0.002	0.497	0	8.1	1885	1885	0.176	937.3	3795.2	2019.6	438	348	0.995	182.7	17871.2	18928.2	1926	1925	0.243	82.56	451	511.35	2	53
87	86	0.002	0.497	0	9.57	1885	1885	0.174	937.3	3780.6	2013.7	422	346	0.996	173.8	17763.8	18819	1944	1944	0.246	85.6	469.7	529.97	3	53
77	76	0.001	0.497	0	8.11	1885	1885	0.176	937.3	3792.4	2026	424	353	0.996	174.4	17589	18624.1	1955	1955	0.246	85.99	468.9	528.83	4	53
81	80	0.001	0.497	0	7.7	1885	1885	0.174	937.3	3736.8	1995.8	419	352	0.996	173	18079.8	19140.9	1950	1949	0.247	94.25	516.4	576.81	5	53
88	88	0.002	0.497	0	8.34	1885	1885	0.176	937.3	3787.3	2020.3	427	353	0.996	177.7	17929.4	18973.2	1947	1946	0.245	80.7	438.5	498.52	6	53
73	72	0.001	0.497	0	7.52	1885	1885	0.174	937.3	3711.6	1973.8	426	349	0.995	177.1	17915	18959.5	1934	1934	0.243	84.28	457.9	517.62	7	53
80	79	0.002	0.497	0	8.87	1885	1885	0.175	937.3	3799.9	2043.6	413	348	0.997	168.1	17598.7	18643.1	1951	1951	0.246	83.43	456.9	516.97	8	53
77	76	0.001	0.497	0	7.43	1885	1885	0.172	937.3	3705.1	1981.9	459	345	0.996	198.4	17830.9	18870.8	1911	1909	0.242	92.35	506.9	567.74	9	53
75	74	0.001	0.497	0	7.49	1885	1885	0.175	937.3	3786.5	2035.8	421	355	0.997	174.6	18212.9	19268	1950	1950	0.244	75.5	408.5	468.04	10	53
75	74	0.001	0.497	0	8.19	1885	1885	0.175	937.3	3753.9	1995.6	268	268	0.739	81.23	9630.03	11417.4	2037	2037	0.257	171.3	939.6	999.66	1	54
74	74	0.001	0.497	0	8.62	1885	1885	0.174	937.3	3717.5	1966.1	250	249	0.68	75.02	8876.21	10682	2021	2021	0.255	174.9	956.4	1016.3	2	54
79	79	0.002	0.497	0	8.39	1885	1885	0.175	937.3	3771.3	2008.6	232	232	0.636	62.66	7365.35	9141.16	2043	2042	0.258	185.5	1017	1077.4	3	54
80	79	0.002	0.497	0	8.97	1885	1885	0.175	937.3	3767	2024	238	238	0.673	70.78	8592.39	10423.7	2041	2041	0.256	183.7	997	1056.7	4	54
78	77	0.001	0.497	0	8.37	1885	1885	0.175	937.3	3757.7	1994.5	264	264	0.755	78.56	9700.79	11555.1	2056	2056	0.26	191.1	1042	1102	5	54
77	76	0.001	0.497	0	7.49	1885	1885	0.175	937.3	3766.1	2014.9	256	255	0.71	76.77	9331.12	11170.7	2033	2033	0.258	183.2	1001	1061.7	6	54
72	72	0.001	0.497	0	8.71	1885	1885	0.174	937.3	3729.4	1984.7	246	245	0.674	73.05	8618.45	10429.9	2022	2021	0.254	174.6	948.7	1008.9	7	54

79	78	0.001	0.497	0	7.48	1885	1885	0.174	937.3	3749.9	2010.6	255	255	0.704	80.03	9668.58	11458.1	2016	2016	0.258	178.4	988.9	1049.8	8	54
77	77	0.002	0.497	0	9	1885	1885	0.173	937.3	3732	2002	265	265	0.735	82.28	10055.1	11853.5	2044	2043	0.255	168.9	910.7	970.53	9	54
75	74	0.001	0.497	0	8.4	1885	1885	0.176	937.3	3773.1	2018.4	279	276	0.761	82.16	9750.48	11626.2	2047	2047	0.259	173.1	941.2	1001.3	10	54
82	82	0.002	0.497	0	8.39	1885	1885	0.174	937.3	3726.9	1989	351	346	0.985	129.6	16053.6	17880.5	2054	2053	0.259	136.1	744.8	805.15	1	55
81	80	0.001	0.497	0	7.37	1885	1885	0.176	937.3	3786.2	2012.7	333	333	0.924	115	13866.3	15664.1	2062	2062	0.258	138.5	753.1	812.5	2	55
76	75	0.001	0.497	0	8.26	1885	1885	0.175	937.3	3784.3	2028.5	341	341	0.96	122.5	15189.9	17013.6	2064	2064	0.261	128.5	706.5	766.62	3	55
82	81	0.002	0.497	0	8.09	1885	1885	0.175	937.3	3773.7	2013.3	353	344	0.993	120.6	14945.1	16803	2060	2059	0.261	139.5	770.7	831.23	4	55
66	66	0.001	0.496	0	8.12	1885	1885	0.175	937.3	3767.9	2012.7	347	347	0.958	125.5	14903.5	16692.2	2055	2054	0.262	135.6	749.5	810.35	5	55
73	73	0.001	0.497	0	8.33	1885	1885	0.175	937.3	3739.2	1990.4	342	341	0.957	113.7	13788.3	15642.5	2076	2075	0.262	148.7	808.7	869.22	6	55
79	78	0.002	0.497	0	9.1	1885	1885	0.173	937.3	3731.3	1992.7	353	353	0.963	125.3	14858.3	16626.3	2058	2058	0.261	134	735.4	795.68	7	55
78	77	0.001	0.497	0	7.41	1885	1885	0.174	937.3	3744.8	1999	329	329	0.919	114.4	13637.3	15448.2	2062	2062	0.261	150.2	819	879.07	8	55
73	73	0.001	0.497	0	8.62	1885	1885	0.174	937.3	3739.4	1993.9	344	343	0.959	121.4	14796.2	16647.7	2068	2067	0.261	141	766.6	827.05	9	55
79	78	0.001	0.497	0	7.57	1885	1885	0.174	937.3	3756.8	2012.9	367	360	0.991	129.4	15591.8	17405.5	2085	2085	0.263	139.3	761.8	821.79	10	55
75	74	0.001	0.497	0	8.5	1885	1885	0.176	937.3	3795	2024.1	304	303	0.827	103.8	12259.1	14065.5	1897	1897	0.238	103	557.3	616.8	1	56
82	81	0.001	0.497	0	7.94	1885	1885	0.174	937.3	3750.8	2002.1	267	266	0.738	81.53	9728.65	11560.7	1910	1910	0.241	141.6	773.9	833.98	2	56
88	87	0.002	0.497	0	7.81	1885	1885	0.175	937.3	3740	1990	280	259	0.723	84.08	10029.1	11869.8	1926	1926	0.242	129.9	701.5	761.17	3	56
73	72	0.001	0.497	0	7.91	1885	1885	0.173	937.3	3721.9	1991	263	261	0.743	82.8	10478.4	12396.4	1925	1925	0.243	144.3	784.6	844.75	4	56
73	72	0.002	0.497	0	9.13	1885	1885	0.175	937.3	3770.3	2011.9	243	243	0.685	81.16	9739.79	11565.4	1925	1925	0.244	140.4	769.8	830.14	5	56
82	81	0.001	0.497	0	7.11	1885	1885	0.174	937.3	3757	2008.8	272	271	0.756	89.99	10749.3	12591.7	1913	1913	0.243	124.2	684.4	744.77	6	56
78	78	0.002	0.497	0	8.53	1885	1885	0.173	937.3	3712.7	1969	259	259	0.704	81.33	9827.2	11588.7	1920	1919	0.241	136.9	740.7	800.69	7	56
75	75	0.001	0.497	0	8.1	1885	1885	0.174	937.3	3757.7	2013.2	266	266	0.733	82.48	9904.43	11689.1	1912	1911	0.242	132.1	724	784.64	8	56
82	81	0.002	0.497	0	8.76	1885	1885	0.175	937.3	3753	2000.7	254	254	0.724	80.13	9880.52	11728.3	1917	1917	0.243	131	723.5	783.71	9	56
75	75	0.001	0.497	0	7.65	1885	1885	0.176	937.3	3778.8	2010.4	260	259	0.72	81.88	9863.26	11696.8	1934	1933	0.242	131	704.4	764.24	10	56
103	102	0.002	0.498	0	8.43	1885	1885	0.176	937.3	3793.1	2024.5	179	178	0.474	35.29	4074.8	5807.6	1956	1956	0.247	171.4	937.4	997.42	1	57
103	102	0.002	0.498	0	8.15	1885	1885	0.175	937.3	3747.9	1977	176	175	0.479	41.54	4965.55	6758.01	1955	1955	0.248	178.3	981.2	1041.5	2	57
103	102	0.002	0.498	0	8.27	1885	1885	0.173	937.3	3714.7	1980.9	180	159	0.43	36.47	4134.35	5911.88	1955	1955	0.245	184.7	999.6	1059.2	3	57
103	102	0.002	0.498	0	7.48	1885	1885	0.177	937.3	3798.6	2013.2	180	179	0.501	42.75	5129.2	6961.14	1954	1954	0.246	172	934.4	994.15	4	57
103	102	0.002	0.498	0	7.23	1885	1885	0.175	937.3	3780.9	2008	158	156	0.43	33.19	4027.97	5849.93	1962	1961	0.249	188.4	1034	1094.8	5	57
103	102	0.002	0.498	0	7.57	1885	1885	0.174	937.3	3772.4	2025.6	180	159	0.431	38.47	4576.39	6353.19	1956	1956	0.248	181.7	994.4	1054.5	6	57
103	102	0.002	0.498	0	8.06	1885	1885	0.175	937.3	3777.1	2022.6	163	163	0.478	38.11	4838.4	6738.72	1961	1961	0.248	181.1	997.9	1058	7	57
103	102	0.002	0.498	0	8.35	1885	1885	0.173	937.3	3706.5	1966.4	149	149	0.393	29.86	3356.87	5066.96	1965	1965	0.248	199.5	1088	1147.7	8	57
103	102	0.002	0.498	0	7.98	1885	1885	0.173	937.3	3738.6	1995.8	153	152	0.419	31.63	3689.8	5494.99	1957	1957	0.247	193.4	1056	1116.5	9	57
103	102	0.002	0.498	0	9.16	1885	1885	0.176	937.3	3770.2	2015.9	132	132	0.348	23.82	2711.38	4419.66	1956	1956	0.247	197.4	1073	1132.7	10	57
20	20	4E-04	0.488	0	7.81	1885	1885	0.175	937.3	3800.1	2045.8	381	345	0.996	150.7	17294.3	18353.6	1922	1921	0.242	73.17	398.1	458.28	1	58
28	28	6E-04	0.491	0	9.2	1885	1885	0.176	937.3	3797.6	2043.2	393	351	0.995	156.5	17592.8	18641.3	1903	1902	0.241	74.06	408.4	468.9	2	58
27	27	6E-04	0.491	0	9.11	1885	1885	0.175	937.3	3770.6	2011.2	407	345	0.996	164.4	18160.3	19245.1	1891	1889	0.242	78.98	436.4	497.74	3	58

29	28	5E-04	0.492	0	7.47	1885	1885	0.176	937.3	3795.6	2030	399	345	0.997	164.9	17967.9	19038.1	1894	1894	0.241	64.5	354.8	415.33	4	58
20	20	4E-04	0.488	0	8.64	1885	1885	0.174	937.3	3741.2	1997.9	413	349	0.997	175.7	18123.9	19179.7	1888	1886	0.236	63.78	344.5	404.33	5	58
33	33	6E-04	0.493	0	8.35	1885	1885	0.174	937.3	3744.2	1997	392	354	0.997	152	17544.6	18588.3	1915	1914	0.241	81.67	444.8	504.86	6	58
37	37	8E-04	0.493	0	9.09	1885	1885	0.175	937.3	3788	2038.1	367	343	0.996	141.2	17119.5	18243.2	1934	1933	0.243	67.53	367.6	427.63	7	58
27	27	4E-04	0.491	0	7.03	1885	1885	0.174	937.3	3788.3	2026.8	409	348	0.998	169.8	18110.7	19177.7	1898	1897	0.239	65.53	354.4	414.47	8	58
24	23	4E-04	0.49	0	7.63	1885	1885	0.175	937.3	3777.5	2020.8	396	353	0.997	156.7	17521.9	18564.8	1902	1902	0.24	74.87	410.9	470.96	9	58
25	25	4E-04	0.49	0	6.76	1885	1885	0.174	937.3	3747.2	1989.6	378	361	0.997	144.7	17134	18707.7	1930	1928	0.245	76.87	421.5	482.27	10	58
27	26	6E-04	0.491	0	9.22	1885	1885	0.175	937.3	3765.2	2007.8	250	250	0.712	83.66	10378.6	12225.4	1919	1919	0.241	123.6	673.4	733.02	1	59
30	30	5E-04	0.492	0	7.9	1885	1885	0.174	937.3	3750.6	1999.8	258	258	0.718	84.55	10173.2	11975.7	1899	1898	0.238	136.3	740.8	800.83	2	59
19	19	4E-04	0.487	0	8.5	1885	1885	0.175	937.3	3792	2034.6	272	272	0.752	96.06	11419.4	13209.7	1910	1909	0.24	114.2	622.2	682.34	3	59
29	29	5E-04	0.492	0	7.47	1885	1885	0.175	937.3	3788.5	2033.2	248	248	0.705	80.23	10198.4	12041.1	1908	1907	0.241	125	685.3	745.78	4	59
39	38	7E-04	0.494	0	7.48	1885	1885	0.173	937.3	3748.4	2017.5	240	240	0.673	75.69	9267.34	11084.9	1925	1925	0.242	145.1	785.3	845.07	5	59
25	25	5E-04	0.49	0	8.69	1885	1885	0.173	937.3	3725.8	1986.5	250	250	0.696	81.06	9734.54	11537.7	1902	1901	0.241	137.4	751.8	812.33	6	59
23	23	4E-04	0.489	0	8.13	1885	1885	0.174	937.3	3768.4	2028.1	237	237	0.637	73.25	8490.45	10233	1921	1920	0.243	149	811.2	871.72	7	59
21	20	4E-04	0.488	0	9.25	1885	1885	0.175	937.3	3755.8	1997.8	219	219	0.607	67.12	8049.7	9844.8	1928	1928	0.243	143.8	790.8	830.84	8	59
27	27	6E-04	0.491	0	8.81	1885	1885	0.175	937.3	3748.1	1991.1	230	230	0.644	72.83	8676.06	10491.7	1932	1931	0.242	142.5	768.9	828.81	9	59
16	16	3E-04	0.485	0	7.41	1885	1885	0.175	937.3	3747.6	2002.5	241	241	0.669	82.13	10085.8	11884	1911	1910	0.243	141.9	776.3	837.21	10	59
26	26	4E-04	0.491	0	6.13	1885	1885	0.175	937.3	3782.5	2027.8	319	319	0.892	113.5	13865	15677	2078	2077	0.262	139.9	762.6	822.96	1	60
31	30	7E-04	0.492	0	9.61	1885	1885	0.175	937.3	3761.8	2005.1	321	321	0.9	114.8	13969.2	15785.3	2075	2075	0.259	134.4	725	784.3	2	60
29	29	5E-04	0.492	0	7.91	1885	1885	0.174	937.3	3737.7	1997.8	345	345	0.905	120.1	13622.5	15323	2082	2081	0.266	147.4	804.1	865.32	3	60
20	20	5E-04	0.488	0	9.76	1885	1885	0.175	937.3	3773.2	2030.4	373	346	0.996	139.8	16519.6	17794.8	2077	2076	0.259	122	655.7	715.4	4	60
33	32	6E-04	0.493	0	8.65	1885	1885	0.173	937.3	3727.2	1984.3	320	319	0.892	108.4	12987.9	14839.9	2094	2094	0.267	164.4	903.4	963.96	5	60
20	20	3E-04	0.488	0	7.41	1885	1885	0.174	937.3	3745.1	2001.6	323	323	0.899	117.3	13805.3	15608.1	2087	2086	0.262	142.2	780.7	840.78	6	60
31	31	5E-04	0.492	0	7.04	1885	1885	0.175	937.3	3781.8	2034.3	336	336	0.924	121.6	14342.5	16124.8	2074	2073	0.262	133.1	718.3	778.6	7	60
33	33	6E-04	0.493	0	7.29	1885	1885	0.174	937.3	3728.6	1978.9	327	327	0.909	116.8	14070.5	15872.6	2075	2074	0.261	139.5	762.8	822.97	8	60
23	23	4E-04	0.489	0	7.07	1885	1885	0.175	937.3	3749.9	1990.8	335	335	0.957	120.5	14876	16726.4	2075	2073	0.265	151.2	831.5	893.03	9	60
25	24	4E-04	0.49	0	7.38	1885	1885	0.175	937.3	3762.6	2013	343	340	0.979	123.5	15329	17111.5	2090	2090	0.265	142.2	777.3	837.65	10	60
29	29	6E-04	0.492	0	9.16	1885	1885	0.175	937.3	3800.8	2044	476	340	0.997	206.5	17820.7	18868.4	1830	1848	0.232	62.64	341.3	401.28	1	61
28	28	6E-04	0.491	0	9.73	1885	1885	0.176	937.3	3815.7	2049.5	491	350	0.997	217.1	18493.3	19539.8	1843	1840	0.232	60.79	331.9	392.29	2	61
30	30	5E-04	0.492	0	7.18	1885	1885	0.173	937.3	3716.8	1990.1	473	351	0.998	206.7	17822	18838.9	1863	1862	0.236	90.97	496.8	557.39	3	61
22	22	4E-04	0.489	0	6.93	1885	1885	0.175	937.3	3772.7	2019.6	469	350	0.997	202.3	17658.1	18678.1	1874	1873	0.237	82.51	450.1	510.32	4	61
23	22	4E-04	0.489	0	7.43	1885	1885	0.174	937.3	3759.2	2010.1	485	361	0.996	211.1	18076.1	19076.8	1866	1866	0.237	66.83	371.2	431.61	5	61
26	26	4E-04	0.491	0	7.47	1885	1885	0.174	937.3	3743.9	1998.1	459	345	0.996	198.6	17942.1	18990.4	1873	1872	0.236	77.95	423.7	483.77	6	61
29	29	6E-04	0.492	0	8.85	1885	1885	0.177	937.3	3804.2	2040.9	479	358	0.996	203.7	17975.9	19003.7	1888	1887	0.24	83.87	458.3	518.95	7	61
19	19	4E-04	0.487	0	10.2	1885	1885	0.177	937.3	3804.5	2036	499	345	0.998	226.6	18284.5	19323.2	1832	1831	0.233	60.16	330.4	390.96	8	61
16	15	3E-04	0.485	0	8.42	1885	1885	0.175	937.3	3761	2010	505	362	0.996	223.4	18023.6	19019.3	1839	1839	0.237	74.29	407.6	468.19	9	61

22	22	5E-04	0.489	0	9.63	1885	1885	0.174	937.3	3749.6	2001.5	457	343	0.996	195.1	17828.8	18880.8	1878	1877	0.236	85.12	461.3	521.22	10	61
22	21	4E-04	0.489	0	8.68	1885	1885	0.175	937.3	3772.7	2017.3	331	330	0.918	119.8	14306.3	16149.2	2049	2049	0.257	111.9	610	669.55	1	62
21	20	3E-04	0.488	0	7.04	1885	1885	0.176	937.3	3772.4	2006.3	346	345	0.947	129	15727.8	17548.4	2051	2051	0.26	122.2	669.5	729.74	2	62
26	26	5E-04	0.491	0	8.42	1885	1885	0.174	937.3	3745.2	1997.6	308	308	0.855	108.4	12992.4	14790.9	2035	2034	0.256	132	718.5	778.57	3	62
34	34	8E-04	0.493	0	9.68	1885	1885	0.176	937.3	3773.4	2012.2	296	296	0.812	103.3	12122.3	13899.7	2027	2026	0.254	136.1	734.6	794.65	4	62
27	27	6E-04	0.491	0	9.1	1885	1885	0.175	937.3	3785	2023.9	328	328	0.895	116.7	13834.6	15603.5	2043	2042	0.257	128.3	697.7	757.99	5	62
20	20	4E-04	0.488	0	8.99	1885	1885	0.174	937.3	3745.4	1999.4	319	319	0.873	116.6	13962.1	15736.3	2028	2027	0.257	125.1	687.9	748.59	6	62
14	13	2E-04	0.483	0	7.78	1885	1885	0.175	937.3	3764.8	2016	316	316	0.86	112.2	13266.2	15030.1	2049	2049	0.257	133.1	722.5	782.21	7	62
24	23	5E-04	0.49	0	9.43	1885	1885	0.175	937.3	3782.2	2033.8	350	348	0.978	130.8	15904.2	17757.2	2029	2028	0.256	109.2	599	659.14	8	62
28	27	5E-04	0.491	0	7.48	1885	1885	0.176	937.3	3757	2003.6	350	348	0.954	121.6	14768.3	16626.3	2048	2048	0.257	132.5	723.9	783.55	9	62
29	29	6E-04	0.492	0	9.29	1885	1885	0.176	937.3	3796.8	2028.6	333	333	0.918	119.9	14397.3	16183	2045	2044	0.257	126.1	691.6	751.77	10	62
27	27	5E-04	0.491	0	7.48	1885	1885	0.175	937.3	3749.6	1996.1	468	349	0.997	210	17793.9	18811.7	1828	1826	0.23	59.27	322.7	382.94	1	63
22	22	4E-04	0.489	0	7.48	1885	1885	0.174	937.3	3754	2007.8	430	352	0.996	176.8	17599.1	18635.6	1893	1892	0.239	83.49	455.8	515.99	2	63
27	27	4E-04	0.491	0	6.62	1885	1885	0.177	937.3	3815.3	2051.5	416	356	0.997	167.5	17935.4	18992.7	1904	1903	0.24	85.06	466.8	527.05	3	63
17	17	3E-04	0.486	0	7.96	1885	1885	0.174	937.3	3749.9	2009.2	457	355	0.997	194.6	17783.1	18806.8	1880	1878	0.237	89.77	491.3	551.81	4	63
25	25	4E-04	0.49	0	7.49	1885	1885	0.175	937.3	3784.4	2034.5	429	357	0.997	178.4	18165.6	19214.4	1885	1885	0.239	82.33	447.3	507.5	5	63
19	19	4E-04	0.487	0	8.36	1885	1885	0.174	937.3	3761.7	2014.6	435	344	0.997	186	18002.7	19055.5	1882	1880	0.238	84.37	461.1	521.69	6	63
30	30	5E-04	0.492	0	7.9	1885	1885	0.175	937.3	3772.9	2021.1	489	363	0.996	217.2	18272.3	19278.9	1842	1839	0.233	62.72	344.1	404.77	7	63
36	36	6E-04	0.493	0	7.78	1885	1885	0.174	937.3	3729	1994.5	446	343	0.996	184.4	17572.1	18618.2	1872	1872	0.236	95.73	517.6	577.58	8	63
28	28	5E-04	0.491	0	7.34	1885	1885	0.175	937.3	3767.9	2012.4	447	354	0.995	185.7	17885.8	18909.7	1865	1864	0.236	75.78	412.7	473.08	9	63
22	22	4E-04	0.489	0	7.05	1885	1885	0.174	937.3	3725.2	1973.2	461	353	0.997	196.3	17538.5	18535.8	1849	1849	0.235	70.54	393.8	454.11	10	63
27	27	4E-04	0.491	0	6.88	1885	1885	0.174	937.3	3735.2	1993.8	557	349	0.996	253.5	18097.3	19111.6	1901	1900	0.239	73.8	402.2	462.31	1	64
13	12	3E-04	0.481	0	9.04	1885	1885	0.175	937.3	3786.3	2039.1	541	340	0.996	240.3	18232.8	19311.2	1933	1933	0.243	75.89	413.3	473.15	2	64
26	26	5E-04	0.491	0	8.1	1885	1885	0.175	937.3	3776.1	2013.4	511	347	0.998	220.9	18071.9	19132.1	1963	1962	0.249	92.41	509.9	570.54	3	64
29	28	4E-04	0.492	0	6.65	1885	1885	0.176	937.3	3774.4	2009.3	549	360	0.996	239.6	18418.6	19442	1953	1953	0.247	76.96	420.7	480.83	4	64
18	18	3E-04	0.486	0	8.18	1885	1885	0.172	937.3	3715.1	1992	555	351	0.997	243.8	17841.5	18852.6	1926	1925	0.242	82.2	445.2	505.13	5	64
29	28	6E-04	0.492	0	8.65	1885	1885	0.174	937.3	3766.5	2016.3	568	354	0.997	246.2	17646	18633.2	1919	1919	0.244	80.77	445.5	505.85	6	64
22	21	5E-04	0.489	0	9.78	1885	1885	0.175	937.3	3754.7	2002.7	560	355	0.997	248.7	18095.3	19107.6	1925	1925	0.244	69.36	382.5	442.77	7	64
21	21	3E-04	0.488	0	5.78	1885	1885	0.175	937.3	3756.6	2012.4	541	350	0.997	231.7	17991.9	19031.5	1943	1941	0.245	86.43	469.5	529.87	8	64
22	21	4E-04	0.489	0	8.48	1885	1885	0.174	937.3	3736	1987.3	508	352	0.997	219.9	18045.8	19081.2	1958	1957	0.248	87.85	480	540.39	9	64
25	25	4E-04	0.49	0	6.15	1885	1885	0.174	937.3	3759.6	2022.6	539	351	0.997	237	17726.5	18738.2	1933	1932	0.243	76.31	415.2	475.23	10	64
19	19	4E-04	0.487	0	8.78	1885	1885	0.175	937.3	3764.2	2017.6	391	355	0.994	137.9	15683.3	16967.3	1989	1988	0.25	135.9	736	796.12	1	65
17	17	3E-04	0.486	0	6.82	1885	1885	0.174	937.3	3726.7	1982.4	404	347	0.994	145.8	16085.6	17415.3	1983	1981	0.251	136.6	751.1	812.13	2	65
28	28	4E-04	0.491	0	6.27	1885	1885	0.173	937.3	3738.7	1998.2	406	339	0.995	146.1	16048.8	17393.9	1982	1980	0.254	146.2	813.2	874.88	3	65
24	24	5E-04	0.49	0	8.34	1885	1885	0.174	937.3	3755.7	2006.3	408	352	0.995	142.7	15583.8	16924.9	1981	1980	0.25	141.7	768.2	828.54	4	65
25	24	4E-04	0.49	0	8.03	1885	1885	0.173	937.3	3710.7	1983	381	353	0.997	127.2	15023.5	16434	2019	2019	0.254	146.6	792.2	851.9	5	65

21	21	4E-04	0.488	0	8.81	1885	1885	0.174	937.3	3752.9	2010.9	399	356	0.995	143.4	15893.2	17207.2	1980	1979	0.247	128.9	691.2	750.81	6	65
29	29	5E-04	0.492	0	7.99	1885	1885	0.175	937.3	3769	2000.2	383	347	0.995	126	14874.6	16302.5	2023	2022	0.257	153.3	839.6	900.32	7	65
33	33	6E-04	0.493	0	7.82	1885	1885	0.175	937.3	3768.5	2009.5	399	349	0.995	142	15935.5	17275.2	1997	1996	0.256	136.4	755.6	816.95	8	65
24	23	4E-04	0.49	0	6.97	1885	1885	0.176	937.3	3796.1	2039.3	390	355	0.995	132.1	15121.1	16450.2	1993	1993	0.251	132.3	718.6	778.47	9	65
21	21	5E-04	0.488	0	9.54	1885	1885	0.174	937.3	3744.1	2000.7	394	368	0.995	131	14894.9	16259.8	2022	2021	0.254	144.3	785.1	845.36	10	65

Point of Entry								Holding Area								Inspection Center								Crane Loading								Est Time (Hours)	Est #	Est Mtr
Entry	Duty Entry	Clean Shift	Duty Shift	Clean Pass	Duty Pass	Clean Fail	Duty Fail	Clean Entry	Duty Entry	Clean Shift	Duty Shift	Clean Pass	Duty Pass	Clean Fail	Duty Fail	Clean Entry	Duty Entry	Clean Shift	Duty Shift	Clean Pass	Duty Pass	Clean Hold	Duty Hold	Clean Entry	Duty Entry	Clean Shift	Duty Shift	Clean Load	Duty Load	Clean Fail	Duty Fail			
101	2	101	2	93	0	7	2	1875	10	1875	10	1790	2	85	8	291	11	291	11	291	11	0	0	1975	12	1975	12	1975	12	0	0	43200	1	1
101	2	101	2	91	0	9	2	1875	10	1875	10	1774	1	101	9	313	11	313	11	313	11	0	0	1975	12	1975	12	1975	12	0	0	43200	2	1
101	2	101	2	92	0	8	2	1875	10	1875	10	1772	0	103	10	301	12	301	12	301	12	0	0	1975	12	1975	12	1975	12	0	0	43200	3	1
101	2	101	2	90	0	10	2	1875	10	1875	10	1776	1	99	9	301	11	301	11	301	11	0	0	1975	12	1975	12	1975	12	0	0	43200	4	1
101	2	101	2	89	0	11	2	1875	10	1875	10	1794	2	81	8	308	11	308	11	308	11	0	0	1975	12	1975	12	1975	12	0	0	43200	5	1
101	2	101	2	94	0	6	2	1875	10	1875	10	1770	0	105	10	333	12	333	12	333	12	0	0	1975	12	1975	12	1975	12	0	0	43200	6	1
101	2	101	2	94	0	6	2	1875	10	1875	10	1769	1	106	9	308	11	308	11	308	11	0	0	1975	12	1975	12	1975	12	0	0	43200	7	1
101	2	101	2	88	0	12	2	1875	10	1875	10	1777	1	98	9	294	11	294	11	294	11	0	0	1975	12	1975	12	1975	12	0	0	43200	8	1
101	2	101	2	93	0	7	2	1875	10	1875	10	1792	0	83	10	279	12	279	12	279	12	0	0	1975	12	1975	12	1975	12	0	0	43200	9	1
101	2	101	2	94	0	6	2	1875	10	1875	10	1783	0	92	10	303	12	303	12	303	12	0	0	1975	12	1975	12	1975	12	0	0	43200	10	1
101	2	101	2	94	1	6	1	1875	10	1875	10	1785	1	90	9	302	10	302	10	221	0	79	10	1894	2	1894	2	1894	2	0	0	43200	1	2
101	2	101	2	97	2	3	0	1875	10	1875	10	1779	0	96	10	318	11	318	11	236	0	81	11	1893	1	1893	1	1893	1	0	0	43200	2	2
101	2	101	2	94	0	6	2	1875	10	1875	10	1769	0	106	10	326	12	326	12	280	0	66	12	1909	0	1909	0	1909	0	0	0	43200	3	2
101	2	101	2	97	0	3	2	1875	10	1875	10	1803	0	72	10	291	12	291	12	217	0	73	12	1901	0	1901	0	1901	0	0	0	43200	4	2
101	2	101	2	97	0	3	2	1875	10	1875	10	1798	0	77	10	328	12	328	12	244	0	84	12	1891	0	1891	0	1891	0	0	0	43200	5	2
101	2	101	2	97	0	3	2	1875	10	1875	10	1769	1	106	9	317	11	317	11	240	0	77	11	1898	1	1898	1	1898	1	0	0	43200	6	2
101	2	101	2	94	0	6	2	1875	10	1875	10	1778	0	97	10	329	12	329	12	244	0	84	12	1890	0	1890	0	1890	0	0	0	43200	7	2
101	2	101	2	96	0	4	2	1875	10	1875	10	1794	1	81	9	284	11	284	11	207	0	76	11	1898	1	1898	1	1898	1	0	0	43200	8	2
101	2	101	2	94	0	6	2	1875	10	1875	10	1788	0	87	10	293	12	293	12	210	0	83	12	1892	0	1892	0	1892	0	0	0	43200	9	2
101	2	101	2	97	1	3	1	1875	10	1875	10	1793	0	82	10	319	11	319	11	249	0	69	11	1905	1	1905	1	1905	1	0	0	43200	10	2
101	2	101	2	95	0	5	2	1875	10	1875	10	1778	0	97	10	443	12	366	12	323	2	28	10	1977	2	1977	2	1854	2	122	0	43200	1	3
101	2	101	2	93	0	7	2	1875	10	1875	10	1784	1	91	9	433	11	339	11	326	2	18	9	1974	3	1974	3	1888	3	106	0	43200	2	3
101	2	101	2	91	0	9	2	1875	10	1875	10	1779	1	96	9	420	12	339	12	323	1	21	11	1979	1	1979	1	1876	1	101	0	43200	3	3
101	2	101	2	92	0	8	2	1875	10	1875	10	1796	1	79	9	416	11	354	11	317	2	22	9	1976	3	1976	3	1874	3	100	0	43200	4	3
101	2	101	2	96	0	4	2	1875	10	1875	10	1798	1	77	9	441	12	380	12	314	2	31	10	1952	3	1952	3	1848	2	104	1	43200	5	3
101	2	101	2	97	0	3	2	1875	10	1875	10	1780	1	95	9	413	11	348	11	308	3	25	8	1966	4	1966	4	1869	4	96	0	43200	6	3

101	2	101	2	96	0	4	2	1875	10	1875	10	1782	0	93	10	425	12	346	12	309	1	22	11	1956	1	1956	1	1839	1	97	0	43200	7	3
101	2	101	2	96	0	4	2	1875	10	1875	10	1786	0	89	10	430	12	347	12	305	3	27	9	1955	3	1955	3	1849	3	105	0	43200	8	3
101	2	101	2	95	1	5	1	1875	10	1875	10	1797	2	78	8	428	10	351	10	317	2	19	8	1968	4	1968	4	1864	4	104	0	43200	9	3
101	2	101	2	98	0	2	2	1875	10	1875	10	1791	1	84	9	417	11	366	11	328	2	23	9	1968	3	1968	3	1885	3	82	0	43200	10	3
101	2	101	2	97	0	3	2	1875	10	1875	10	1789	1	86	9	378	12	362	12	265	0	82	12	1978	0	1978	0	1862	0	116	0	43200	1	4
101	2	101	2	99	1	1	1	1875	10	1875	10	1783	0	92	10	379	11	348	11	249	0	84	11	1954	1	1954	1	1845	1	109	0	43200	2	4
101	2	101	2	96	0	4	2	1875	10	1875	10	1784	1	91	9	370	12	354	11	242	0	97	11	1933	1	1933	1	1847	1	86	0	43200	3	4
101	2	101	2	97	0	3	2	1875	10	1875	10	1767	1	108	9	384	11	356	11	250	1	91	10	1942	2	1942	2	1841	2	101	0	43200	4	4
101	2	101	2	94	0	6	2	1875	10	1875	10	1773	2	102	8	396	10	371	10	261	0	95	10	1948	2	1948	2	1840	2	108	0	43200	5	4
101	2	101	2	96	0	4	2	1875	10	1875	10	1790	1	85	9	365	11	348	11	241	0	92	11	1939	1	1939	1	1850	1	88	0	43200	6	4
101	2	101	2	96	0	4	2	1875	10	1875	10	1786	1	89	9	354	11	354	11	261	0	85	11	1972	1	1972	1	1882	1	90	0	43200	7	4
101	2	101	2	95	0	5	2	1875	10	1875	10	1772	0	103	10	411	12	350	12	258	0	77	12	1939	0	1939	0	1822	0	117	0	43200	8	4
101	2	101	2	96	0	4	2	1875	10	1875	10	1781	0	94	10	403	12	355	12	254	0	86	12	1935	0	1935	0	1826	0	109	0	43200	9	4
101	2	101	2	95	0	5	2	1875	10	1875	10	1804	2	71	8	369	10	350	10	257	0	78	10	1982	2	1982	2	1862	2	119	0	43200	10	4
101	2	101	2	95	0	5	2	1875	10	1875	10	1788	0	87	10	273	12	273	12	258	6	15	6	2021	6	2021	6	1960	6	61	0	43200	1	5
101	2	101	2	94	0	6	2	1875	10	1875	10	1770	1	105	9	294	12	294	12	276	5	17	7	2023	6	2023	6	1957	5	66	1	43200	2	5
101	2	101	2	100	0	0	2	1875	10	1875	10	1774	2	101	8	291	12	291	12	271	4	20	8	2020	6	2020	6	1955	4	65	2	43200	3	5
101	2	101	2	100	0	0	2	1875	10	1875	10	1795	0	80	10	278	12	278	12	264	5	14	7	2027	5	2027	5	1961	5	66	0	43200	4	5
101	2	101	2	99	0	1	2	1875	10	1875	10	1785	0	89	10	297	12	297	12	271	7	25	5	2025	7	2025	7	1949	7	76	0	43200	5	5
101	2	101	2	95	0	5	2	1875	10	1875	10	1791	1	84	9	271	12	271	12	248	4	21	8	2016	5	2016	5	1952	4	64	1	43200	6	5
101	2	101	2	100	0	0	2	1875	10	1875	10	1790	0	85	10	265	12	265	12	251	5	14	7	2041	5	2041	5	1961	5	80	0	43200	7	5
101	2	101	2	98	1	2	1	1875	10	1875	10	1763	3	112	7	304	12	304	12	293	6	11	6	2042	10	2042	10	1964	6	78	4	43200	8	5
101	2	101	2	97	0	3	2	1875	10	1875	10	1779	0	96	10	281	12	281	12	262	6	19	6	2019	6	2019	6	1956	6	63	0	43200	9	5
101	2	101	2	99	0	1	2	1875	10	1875	10	1784	2	91	8	271	12	271	12	254	7	15	5	2022	9	2022	9	1958	7	64	2	43200	10	5
101	2	101	2	100	2	0	0	1875	10	1875	10	1796	0	79	10	236	12	236	12	180	0	56	12	1990	2	1990	2	1919	0	71	2	43200	1	6
101	2	101	2	99	2	1	0	1875	10	1875	10	1778	2	97	8	294	12	294	12	209	0	85	12	1982	4	1982	4	1890	0	92	4	43200	2	6
101	2	101	2	98	2	2	0	1875	10	1875	10	1782	1	93	9	241	12	241	12	177	0	64	12	1976	3	1976	3	1911	0	65	3	43200	3	6
101	2	101	2	100	2	0	0	1875	10	1875	10	1771	0	104	10	259	12	259	12	193	0	66	12	1974	2	1974	2	1909	0	65	2	43200	4	6
101	2	101	2	98	2	2	0	1875	10	1875	10	1795	4	80	6	231	12	231	12	171	0	58	12	1981	6	1981	6	1915	0	66	6	43200	5	6
101	2	101	2	98	2	2	0	1875	10	1875	10	1770	1	105	9	275	11	275	11	202	0	73	11	1989	2	1989	2	1902	1	67	1	43200	6	6
101	2	101	2	100	2	0	0	1875	10	1875	10	1787	0	88	10	262	12	262	12	185	1	77	11	1972	3	1972	3	1898	1	74	2	43200	7	6
101	2	101	2	99	2	1	0	1875	10	1875	10	1788	2	107	8	280	12	280	12	217	0	62	12	1983	4	1983	4	1912	0	71	4	43200	8	6
101	2	101	2	99	2	1	0	1875	10	1875	10	1796	0	79	10	264	12	264	12	186	0	78	12	1984	2	1984	2	1897	0	87	2	43200	9	6
101	2	101	2	100	2	0	0	1875	10	1875	10	1792	1	83	9	244	12	244	12	177	0	67	12	1978	3	1978	3	1908	0	70	3	43200	10	6
101	2	101	2	99	0	1	2	1875	10	1875	10	1774	1	101	9	354	12	354	12	330	2	11	10	2107	3	2107	3	1950	2	156	1	43200	1	7
101	2	101	2	97	0	3	2	1875	10	1875	10	1793	1	82	9	338	12	338	12	326	0	12	12	2132	1	2132	1	1963	0	169	1	43200	2	7
101	2	101	2	98	1	2	1	1875	10	1875	10	1776	1	99	9	361	12	352	12	329	2	8	10	2111	4	2111	4	1943	2	168	2	43200	3	7
101	2	101	2	100	0	0	2	1875	10	1875	10	1789	0	86	10	356	12	350	12	328	3	7	9	2119	3	2119	3	1945	3	172	0	43200	4	7
101	2	101	2	98	0	2	2	1875	10	1875	10	1789	0	86	10	356	12	351	12	327	1	9	11	2126	1	2126	1	1946	1	180	0	43200	5	7
101	2	101	2	96	0	4	2	1875	10	1875	10	1791	0	84	10	332	12	332	12	316	0	15	12	2129	0	2129	0	1959	0	170	0	43200	6	7
101	2	101	2	97	0	3	2	1875	10	1875	10	1782	0	93	10	346	12	346	12	338	0	7	12	2129	0	2129	0	1967	0	162	0	43200	7	7
101	2	101	2	99	0	2	2	1875	10	1875	10	1786	2	89	8	359	12	350	12	326	1	9	11	2118	3	2118	3	1942	1	175	2	43200	8	7
101	2	101	2	100	1	1	1	1875	10	1875	10	1777	1	98	9	350	12	350	12	326	0	10	12	2116	2	2116	2	1951	0	164	2	43200	9	7

101	2	101	2	98	1	2	1	1875	10	1875	10	1759	0	116	10	399	12	332	12	325	4	12	8	2080	5	2080	5	1901	4	179	1	43200	10	7
101	2	101	2	101	2	0	0	1875	10	1875	10	1790	1	85	9	353	12	347	12	280	1	72	11	2040	4	2040	4	1882	1	157	3	43200	1	8
101	2	101	2	101	2	0	0	1875	10	1875	10	1780	0	95	10	391	12	338	12	280	1	83	11	2030	3	2030	3	1844	1	185	2	43200	2	8
101	2	101	2	101	2	0	0	1875	10	1875	10	1784	1	91	9	396	12	338	12	280	0	83	12	2036	3	2036	3	1839	0	186	3	43200	3	8
101	2	101	2	101	2	0	0	1875	10	1875	10	1793	1	82	9	383	11	355	11	256	1	84	10	2032	4	2032	4	1847	2	183	2	43200	4	8
101	2	101	2	101	2	0	0	1875	10	1875	10	1778	0	97	10	404	12	349	12	255	1	79	11	2016	3	2016	3	1826	1	189	2	43200	5	8
101	2	101	2	101	2	0	0	1875	10	1875	10	1769	1	106	9	395	12	380	12	250	3	95	9	2001	6	2001	6	1829	3	170	3	43200	6	8
101	2	101	2	101	2	0	0	1875	10	1875	10	1787	0	88	10	377	12	330	12	271	0	64	12	2040	1	2040	1	1868	0	170	1	43200	7	8
101	2	101	2	101	2	0	0	1875	10	1875	10	1792	0	83	10	330	12	330	12	272	1	71	11	2053	3	2053	3	1896	1	155	2	43200	8	8
101	2	101	2	101	2	0	0	1875	10	1875	10	1790	0	85	10	368	11	356	11	255	1	86	10	2030	3	2030	3	1861	2	167	1	43200	9	8
101	2	101	2	101	2	0	0	1875	10	1875	10	1787	0	88	10	339	11	339	11	267	1	80	10	2052	3	2052	3	1882	2	168	1	43200	10	8
25	1	25	1	24	0	1	1	1875	10	1875	10	1796	0	79	10	402	12	363	12	281	2	67	10	2017	3	2017	3	1854	2	162	1	43200	1	9
26	2	26	2	24	0	2	2	1875	10	1875	10	1797	1	78	9	446	12	345	12	264	1	66	11	1991	2	1991	2	1792	1	197	1	43200	2	9
40	0	40	0	36	0	3	0	1875	10	1875	10	1797	0	78	10	412	11	349	11	267	0	67	11	2000	2	2000	2	1830	1	170	1	43200	3	9
22	1	22	1	21	0	0	1	1875	10	1875	10	1786	0	89	10	392	12	363	12	280	0	68	12	2015	1	2015	1	1863	0	152	1	43200	4	9
23	1	23	1	22	0	1	1	1875	10	1875	10	1812	0	63	10	373	12	380	12	287	0	58	12	2041	1	2041	1	1887	0	151	1	43200	5	9
29	1	29	1	27	0	2	1	1875	10	1875	10	1801	1	74	9	410	12	339	12	287	0	57	12	2030	2	2030	2	1852	0	177	2	43200	6	9
27	1	27	1	26	0	0	1	1875	10	1875	10	1798	1	77	9	418	11	348	11	277	1	56	10	2011	3	2011	3	1833	2	177	1	43200	7	9
28	1	28	1	27	0	1	1	1875	10	1875	10	1787	1	88	9	443	12	334	12	275	1	64	11	1976	2	1976	2	1807	1	168	1	43200	8	9
26	1	26	1	26	0	0	1	1875	10	1875	10	1796	0	79	10	401	12	344	12	270	0	59	12	2004	1	2004	1	1843	0	159	1	43200	9	9
28	0	28	0	28	0	0	0	1875	10	1875	10	1806	2	69	8	432	12	355	12	276	2	64	10	2001	4	2001	4	1819	2	181	2	43200	10	9
20	0	20	0	18	0	1	0	1875	10	1875	10	1799	1	76	9	525	12	354	12	315	0	24	12	1937	2	1937	2	1765	0	172	2	43200	1	10
29	1	29	1	28	0	1	1	1875	10	1875	10	1798	2	77	8	501	12	361	12	323	0	23	12	1951	3	1951	3	1797	0	153	3	43200	2	10
29	0	29	0	25	0	3	0	1875	10	1875	10	1787	1	88	9	486	11	353	11	316	1	22	10	1956	3	1956	3	1805	2	151	1	43200	3	10
27	1	27	1	26	0	1	1	1875	10	1875	10	1810	1	65	9	488	12	367	12	330	0	22	12	1981	0	1981	0	1818	0	163	0	43200	4	10
26	0	26	0	25	0	1	0	1875	10	1875	10	1797	1	78	9	487	12	342	12	299	0	28	12	1953	3	1953	3	1785	0	165	3	43200	5	10
35	1	35	1	34	0	1	1	1875	10	1875	10	1797	0	78	10	498	12	352	12	297	1	40	11	1929	1	1929	1	1773	1	154	0	43200	6	10
27	1	27	1	25	0	2	1	1875	10	1875	10	1799	1	76	9	497	12	353	12	310	0	28	12	1939	1	1939	1	1789	0	150	1	43200	7	10
26	1	26	1	23	1	3	0	1875	10	1875	10	1793	0	82	10	494	12	365	12	317	1	33	11	1945	3	1945	3	1799	1	146	2	43200	8	10
22	2	22	2	20	0	2	2	1875	10	1875	10	1810	0	65	10	466	12	348	12	306	0	27	12	1956	0	1956	0	1815	0	140	0	43200	9	10
28	1	28	1	27	1	0	0	1875	10	1875	10	1809	1	66	9	446	12	349	12	311	1	23	11	1989	3	1989	3	1840	1	149	2	43200	10	10
24	1	24	1	24	0	0	1	1875	10	1875	10	1796	3	79	7	375	12	336	12	247	0	74	12	1909	4	1909	4	1846	0	61	4	43200	1	11
26	0	26	0	25	0	0	0	1875	10	1875	10	1786	1	89	9	429	12	347	12	245	0	87	12	1856	3	1856	3	1791	0	65	3	43200	2	11
27	2	27	2	27	0	0	2	1875	10	1875	10	1816	1	59	9	382	12	356	12	261	0	80	12	1915	0	1915	0	1854	0	60	0	43200	3	11
30	0	30	0	30	0	0	0	1875	10	1875	10	1801	0	74	10	384	12	380	12	268	0	77	12	1926	2	1926	2	1857	0	66	2	43200	4	11
19	0	19	0	18	0	1	0	1875	10	1875	10	1793	0	82	10	394	12	356	12	261	0	80	12	1908	1	1908	1	1842	0	65	1	43200	5	11
22	1	22	1	20	0	2	1	1875	10	1875	10	1806	0	69	10	411	12	348	12	255	0	78	12	1884	1	1884	1	1819	0	64	1	43200	6	11
21	0	21	0	19	0	2	0	1875	10	1875	10	1806	0	69	10	402	12	338	12	272	0	71	12	1924	2	1924	2	1846	0	78	2	43200	7	11
27	0	27	0	25	0	2	0	1875	10	1875	10	1806	1	69	9	398	11	351	11	259	0	77	11	1898	3	1898	3	1836	1	61	2	43200	8	11
29	0	29	0	28	0	1	0	1875	10	1875	10	1806	2	69	8	394	12	353	12	238	1	80	11	1905	5	1905	5	1840	1	65	4	43200	9	11
28	0	28	0	27	0	1	0	1875	10	1875	10	1792	1	83	9	442	11	350	11	249	0	86	11	1851	3	1851	3	1782	1	68	2	43200	10	11
21	0	21	0	20	0	1	0	1875	10	1875	10	1816	1	59	9	325	12	325	12	286	2	39	10	2007	4	2007	4	1936	2	70	2	43200	1	12
20	1	20	1	19	0	1	1	1875	10	1875	10	1812	3	63	7	297	12	297	12	280	4	37	8	2017	7	2017	7	1938	4	78	3	43200	2	12

31	1	31	1	30	1	1	0	1875	10	1875	10	1796	0	79	10	286	12	286	12	248	4	37	8	1998	5	1998	5	1937	4	60	1	43200	3	12
23	1	23	1	23	0	0	1	1875	10	1875	10	1807	0	68	10	322	12	322	12	292	3	30	9	2028	3	2028	3	1945	3	82	0	43200	4	12
25	0	25	0	24	0	0	0	1875	10	1875	10	1807	0	68	10	275	12	275	12	239	2	36	10	2000	4	2000	4	1939	2	61	2	43200	5	12
17	0	17	0	16	0	1	0	1875	10	1875	10	1812	0	63	10	290	12	290	12	238	5	31	7	2010	7	2010	7	1943	5	66	2	43200	6	12
30	0	30	0	29	0	0	0	1875	10	1875	10	1803	1	72	9	303	12	303	12	264	1	39	11	1997	4	1997	4	1936	1	61	3	43200	7	12
25	1	25	1	23	0	2	1	1875	10	1875	10	1814	1	61	9	311	12	311	12	278	1	33	11	2007	2	2007	2	1942	1	64	1	43200	8	12
29	1	29	1	28	1	0	0	1875	10	1875	10	1799	1	76	9	323	12	323	12	295	4	28	8	2023	6	2023	6	1946	4	76	2	43200	9	12
26	1	26	1	24	0	2	1	1875	10	1875	10	1797	1	78	9	313	12	313	12	277	4	36	8	2013	6	2013	6	1939	4	73	2	43200	10	12
22	1	22	1	22	0	0	1	1875	10	1875	10	1794	0	81	10	314	11	314	11	232	0	81	11	1996	1	1996	1	1893	1	102	0	43200	1	13
19	0	19	0	19	0	0	0	1875	10	1875	10	1797	2	78	8	291	8	291	8	222	0	69	8	2014	4	2014	4	1906	4	107	0	43200	2	13
19	2	19	2	16	0	2	2	1875	10	1875	10	1777	1	98	9	335	11	335	11	238	1	76	10	1993	2	1993	2	1898	2	95	0	43200	3	13
25	0	25	0	22	0	2	0	1875	10	1875	10	1784	2	91	8	328	8	328	8	251	0	76	8	2004	4	2004	4	1898	4	106	0	43200	4	13
21	1	21	1	21	0	0	1	1875	10	1875	10	1808	2	67	8	334	10	334	10	254	1	79	9	2018	4	2018	4	1895	3	122	1	43200	5	13
21	2	21	2	21	1	0	1	1875	10	1875	10	1802	1	73	9	270	10	270	10	210	0	59	10	2012	2	2012	2	1915	2	96	0	43200	6	13
26	0	26	0	25	0	1	0	1875	10	1875	10	1812	1	63	9	339	9	339	9	261	0	76	9	2031	3	2031	3	1898	3	133	0	43200	7	13
24	1	24	1	24	0	0	1	1875	10	1875	10	1791	2	84	8	309	9	309	9	231	3	77	6	2001	6	2001	6	1898	6	103	0	43200	8	13
30	0	30	0	27	0	2	0	1875	10	1875	10	1800	1	75	9	323	9	323	9	256	1	67	8	2034	4	2034	4	1908	4	126	0	43200	9	13
29	0	29	0	29	0	0	0	1875	10	1875	10	1803	1	72	9	285	9	285	9	229	0	56	9	2016	3	2016	3	1919	3	96	0	43200	10	13
31	2	31	2	31	2	0	0	1875	10	1875	10	1786	0	89	10	280	10	280	10	228	1	32	9	2042	3	2042	3	1943	3	98	0	43200	1	14
31	1	31	1	30	1	0	0	1875	10	1875	10	1804	1	71	9	246	10	246	10	219	1	27	9	2046	4	2046	4	1948	3	98	1	43200	2	14
22	0	22	0	22	0	0	0	1875	10	1875	10	1795	0	80	10	257	10	257	10	216	1	41	9	2037	3	2037	3	1934	3	102	0	43200	3	14
27	0	27	0	27	0	0	0	1875	10	1875	10	1812	4	63	6	243	6	243	6	218	0	25	6	2044	6	2044	6	1950	6	93	0	43200	4	14
27	0	27	0	27	0	0	0	1875	10	1875	10	1811	0	64	10	261	11	261	11	238	0	23	11	2063	1	2063	1	1952	1	110	0	43200	5	14
27	1	27	1	26	1	1	0	1875	10	1875	10	1795	0	80	10	272	10	272	10	234	1	38	9	2048	3	2048	3	1937	3	110	0	43200	6	14
23	0	23	0	23	0	0	0	1875	10	1875	10	1806	0	69	10	266	10	266	10	236	1	30	9	2070	3	2070	3	1945	3	124	0	43200	7	14
15	1	15	1	15	1	0	0	1875	10	1875	10	1802	3	73	7	276	9	276	9	240	1	35	8	2070	5	2070	5	1939	4	130	1	43200	8	14
29	0	29	0	28	0	1	0	1875	10	1875	10	1811	0	64	10	242	10	242	10	205	1	37	9	2047	3	2047	3	1938	3	108	0	43200	9	14
21	1	21	1	20	1	0	0	1875	10	1875	10	1813	0	62	10	240	10	240	10	216	1	24	9	2055	3	2055	3	1951	3	104	0	43200	10	14
19	0	19	0	19	0	0	0	1875	10	1875	10	1784	1	91	9	172	9	172	9	134	0	38	9	1939	3	1939	3	1937	3	1	0	43200	1	15
22	2	22	2	22	0	0	2	1875	10	1875	10	1799	0	76	10	149	12	149	12	119	0	30	12	1947	0	1947	0	1945	0	1	0	43200	2	15
21	1	21	1	20	1	0	0	1875	10	1875	10	1807	0	68	10	145	10	145	10	115	0	30	10	1946	2	1946	2	1945	2	1	0	43200	3	15
17	2	17	2	16	1	1	1	1875	10	1875	10	1781	1	94	9	191	11	191	11	149	0	42	11	1934	2	1934	2	1933	1	0	1	43200	4	15
25	0	25	0	24	0	0	0	1875	10	1875	10	1810	1	65	9	147	9	147	9	114	1	33	8	1943	4	1943	4	1942	4	1	0	43200	5	15
34	0	34	0	34	0	0	0	1875	10	1875	10	1784	1	91	9	175	9	175	9	138	0	37	9	1940	3	1940	3	1938	3	1	0	43200	6	15
25	0	25	0	25	0	0	0	1875	10	1875	10	1786	1	89	9	163	10	163	10	130	0	33	10	1944	2	1944	2	1942	2	1	0	43200	7	15
23	1	23	1	22	0	1	1	1875	10	1875	10	1803	1	72	9	154	11	154	11	127	0	27	11	1949	2	1949	2	1948	1	0	1	43200	8	15
28	0	28	0	25	0	3	0	1875	10	1875	10	1809	3	66	7	145	7	145	7	106	0	38	7	1938	5	1938	5	1937	5	1	0	43200	9	15
27	1	27	1	25	0	2	1	1875	10	1875	10	1805	1	70	9	154	11	154	11	127	0	27	11	1950	1	1950	1	1948	1	1	0	43200	10	15
25	0	25	0	25	0	0	0	1875	10	1875	10	1805	2	70	8	205	9	205	9	193	8	12	1	1964	12	1964	12	1963	11	0	1	43200	1	16
24	1	24	1	24	1	0	0	1875	10	1875	10	1796	2	79	8	233	9	233	9	216	7	17	2	1962	10	1962	10	1958	10	3	0	43200	2	16
20	0	20	0	20	0	0	0	1875	10	1875	10	1785	0	90	10	225	10	225	10	209	8	16	2	1961	10	1961	10	1959	10	1	0	43200	3	16
28	1	28	1	28	1	0	0	1875	10	1875	10	1803	0	72	10	232	10	232	10	218	8	13	2	1963	10	1963	10	1961	10	1	0	43200	4	16
22	0	22	0	22	0	0	0	1875	10	1875	10	1804	1	71	9	210	9	210	9	198	9	12	0	1965	12	1965	12	1963	12	1	0	43200	5	16

28	1	28	1	28	1	0	0	1875	10	1875	10	1801	0	74	10	218	10	218	10	203	9	15	1	1964	11	1964	11	1980	11	3	0	43200	6	16
21	1	21	1	21	1	0	0	1875	10	1875	10	1802	1	73	9	197	10	197	10	186	7	11	3	1966	9	1966	9	1964	9	1	0	43200	7	16
17	1	17	1	17	1	0	0	1875	10	1875	10	1797	2	78	8	218	8	218	8	210	7	8	1	1969	11	1969	11	1967	11	1	0	43200	8	16
21	1	21	1	21	1	0	0	1875	10	1875	10	1795	0	80	10	201	11	201	11	187	8	13	3	1965	9	1965	9	1961	9	3	0	43200	9	16
23	1	23	1	23	1	0	0	1875	10	1875	10	1813	1	62	9	200	10	200	10	189	9	10	1	1967	11	1967	11	1964	11	2	0	43200	10	16
52	1	52	1	42	0	9	1	1875	10	1875	10	1853	6	22	4	182	7	182	7	176	6	6	1	1975	11	1975	11	1969	11	6	0	43200	1	17
44	1	44	1	39	0	5	1	1875	10	1875	10	1859	7	16	3	176	7	176	7	165	6	11	1	1968	11	1968	11	1964	11	3	0	43200	2	17
48	2	48	2	47	0	1	2	1875	10	1875	10	1858	6	17	4	163	6	163	6	154	4	8	2	1970	10	1970	10	1967	10	3	0	43200	3	17
55	1	55	1	53	0	2	1	1875	10	1875	10	1855	5	20	5	175	6	175	6	166	5	8	1	1974	11	1974	11	1966	11	7	0	43200	4	17
49	2	49	2	43	0	5	2	1875	10	1875	10	1857	6	18	4	175	7	175	7	167	4	8	3	1972	9	1972	9	1967	9	5	0	43200	5	17
55	1	55	1	55	0	0	1	1875	10	1875	10	1856	6	19	4	184	6	184	6	172	5	12	1	1971	11	1971	11	1963	11	7	0	43200	6	17
50	0	50	0	49	0	1	0	1875	10	1875	10	1855	6	20	4	188	6	188	6	178	5	9	1	1973	11	1973	11	1965	11	7	0	43200	7	17
51	1	51	1	48	0	3	1	1875	10	1875	10	1861	8	14	2	184	6	184	6	173	5	10	1	1968	12	1968	12	1964	11	3	1	43200	8	17
65	2	65	2	61	0	3	2	1875	10	1875	10	1856	6	19	4	171	6	171	6	161	4	10	2	1969	10	1969	10	1965	10	4	0	43200	9	17
51	2	51	2	46	0	4	2	1875	10	1875	10	1856	7	18	3	178	7	178	7	163	5	14	2	1963	11	1963	11	1960	10	3	1	43200	10	17
49	1	49	1	48	0	1	1	1875	10	1875	10	1860	7	15	3	298	7	298	7	231	0	67	7	1910	5	1910	5	1908	5	1	0	43200	1	18
58	1	58	1	56	0	2	1	1875	10	1875	10	1856	6	19	4	294	6	294	6	236	0	58	6	1919	6	1919	6	1917	6	1	0	43200	2	18
55	1	55	1	50	1	4	0	1875	10	1875	10	1855	7	20	3	284	7	284	7	214	0	69	7	1906	5	1906	5	1905	5	1	0	43200	3	18
47	0	47	0	44	0	2	0	1875	10	1875	10	1864	6	11	4	304	6	304	6	245	0	59	6	1917	6	1917	6	1916	6	1	0	43200	4	18
48	1	48	1	46	0	1	1	1875	10	1875	10	1847	5	28	5	321	7	321	7	261	0	60	7	1916	5	1916	5	1915	5	1	0	43200	5	18
55	2	55	2	52	0	2	2	1875	10	1875	10	1854	6	21	4	334	6	334	6	235	0	97	6	1877	6	1877	6	1876	6	1	0	43200	6	18
44	1	44	1	40	0	3	1	1875	10	1875	10	1857	6	18	4	337	6	337	6	265	0	70	6	1904	6	1904	6	1903	6	1	0	43200	7	18
55	2	55	2	53	0	2	2	1875	10	1875	10	1849	7	26	3	304	6	304	6	244	0	58	6	1916	7	1916	7	1915	6	0	1	43200	8	18
45	2	45	2	43	0	1	2	1875	10	1875	10	1851	6	24	4	305	8	305	8	241	0	64	8	1912	4	1912	4	1911	4	1	0	43200	9	18
58	0	58	0	56	0	1	0	1875	10	1875	10	1853	6	22	4	341	5	341	5	253	0	88	5	1888	7	1888	7	1887	7	1	0	43200	10	18
48	1	48	1	43	0	5	1	1875	10	1875	10	1855	6	20	4	408	7	363	7	303	2	45	5	1964	7	1964	7	1870	7	93	0	43200	1	19
42	2	42	2	40	0	2	2	1875	10	1875	10	1860	6	15	4	403	8	361	8	304	0	42	8	1965	4	1965	4	1876	4	88	0	43200	2	19
53	1	53	1	48	0	5	1	1875	10	1875	10	1856	6	19	4	391	5	367	5	316	0	36	5	2004	7	2004	7	1900	7	103	0	43200	3	19
50	0	50	0	47	0	2	0	1875	10	1875	10	1862	6	13	4	412	7	362	7	300	0	47	7	1956	6	1956	6	1862	5	93	1	43200	4	19
47	0	47	0	43	0	3	0	1875	10	1875	10	1859	7	16	3	433	7	363	7	306	1	42	6	1965	6	1965	6	1848	6	117	0	43200	5	19
47	1	47	1	45	0	2	1	1875	10	1875	10	1851	6	24	4	380	9	355	9	298	0	42	9	1968	3	1968	3	1892	3	94	0	43200	6	19
44	1	44	1	41	0	3	1	1875	10	1875	10	1862	6	13	4	387	5	370	5	300	0	55	5	1977	7	1977	7	1887	7	88	0	43200	7	19
60	2	60	2	56	0	3	2	1875	10	1875	10	1856	5	19	5	386	7	355	7	301	0	39	7	1978	5	1978	5	1890	5	88	0	43200	8	19
50	2	50	2	48	0	2	2	1875	10	1875	10	1858	7	17	3	376	7	355	7	299	1	41	6	1982	6	1982	6	1899	6	83	0	43200	9	19
49	1	49	1	44	0	5	1	1875	10	1875	10	1864	7	11	3	397	6	363	6	304	3	44	3	1990	9	1990	9	1881	9	107	0	43200	10	19
61	1	61	1	55	1	5	0	1875	10	1875	10	1866	8	9	2	167	2	167	2	126	0	41	2	2046	10	2046	10	1934	10	112	0	43200	1	20
48	1	48	1	44	0	4	1	1875	10	1875	10	1860	6	15	4	180	6	180	6	141	0	39	6	2059	6	2059	6	1936	6	122	0	43200	2	20
52	1	52	1	49	0	2	1	1875	10	1875	10	1855	6	20	4	185	5	185	5	124	1	60	4	2049	8	2049	8	1914	8	135	0	43200	3	20
55	1	55	1	48	1	6	0	1875	10	1875	10	1859	6	16	4	193	4	193	4	154	0	39	4	2068	8	2068	8	1936	8	132	0	43200	4	20
48	0	48	0	46	0	2	0	1875	10	1875	10	1858	5	17	5	180	5	180	5	116	0	43	5	2047	7	2047	7	1931	7	115	0	43200	5	20
50	1	50	1	49	0	0	1	1875	10	1875	10	1852	6	23	4	172	5	172	5	131	0	41	5	2049	7	2049	7	1934	7	115	0	43200	6	20
44	2	44	2	44	0	0	2	1875	10	1875	10	1854	5	21	5	167	7	167	7	127	0	40	7	2048	5	2048	5	1935	5	112	0	43200	7	20
49	0	49	0	48	0	1	0	1875	10	1875	10	1857	7	18	3	154	5	154	5	114	0	38	5	2032	9	2032	9	1935	7	96	2	43200	8	20

54	1	54	1	54	0	0	1	1875	10	1875	10	1842	6	33	4	189	6	189	6	138	1	51	5	2049	8	2049	8	1924	7	124	1	43200	9	20
52	1	52	1	51	0	1	1	1875	10	1875	10	1859	6	16	4	165	5	165	5	126	0	39	5	2048	7	2048	7	1936	7	111	0	43200	10	20
42	2	42	2	41	0	1	2	1875	10	1875	10	1865	7	10	3	343	12	343	12	295	1	38	11	2002	5	2002	5	1927	1	74	4	43200	1	21
54	1	54	1	54	0	0	1	1875	10	1875	10	1858	6	17	4	340	12	340	12	289	2	38	10	1988	7	1988	7	1924	2	63	5	43200	2	21
59	2	59	2	57	1	1	1	1875	10	1875	10	1851	7	24	3	368	10	362	10	316	2	31	8	2006	8	2006	8	1920	4	83	4	43200	3	21
37	0	37	0	37	0	0	0	1875	10	1875	10	1860	7	15	3	333	12	333	12	303	1	28	11	2009	9	2009	9	1945	1	63	8	43200	4	21
54	2	54	2	54	0	0	2	1875	10	1875	10	1858	6	17	4	334	11	334	11	288	2	45	9	1996	7	1996	7	1929	3	66	4	43200	5	21
51	1	51	1	48	0	3	1	1875	10	1875	10	1858	6	17	4	375	12	357	12	309	2	33	10	1993	7	1993	7	1909	2	83	5	43200	6	21
48	2	48	2	46	0	2	2	1875	10	1875	10	1852	6	23	4	370	12	353	12	313	6	25	6	1989	10	1989	10	1918	6	70	4	43200	7	21
47	0	47	0	46	0	1	0	1875	10	1875	10	1847	7	28	3	371	11	354	11	306	3	33	8	1972	10	1972	10	1910	4	61	6	43200	8	21
48	1	48	1	46	0	2	1	1875	10	1875	10	1851	6	24	4	379	12	351	12	300	4	36	8	1970	10	1970	10	1897	4	73	6	43200	9	21
49	2	49	2	46	0	2	2	1875	10	1875	10	1854	6	21	4	382	12	361	12	314	4	32	8	2000	8	2000	8	1906	4	93	4	43200	10	21
51	2	51	2	50	2	0	0	1875	10	1875	10	1861	5	14	5	238	11	238	11	206	0	52	11	1992	7	1992	7	1923	1	69	6	43200	1	22
47	1	47	1	45	1	1	0	1875	10	1875	10	1851	6	24	4	275	10	275	10	211	1	64	9	1985	6	1985	6	1911	3	74	3	43200	2	22
53	2	53	2	53	2	0	0	1875	10	1875	10	1854	7	21	3	280	12	280	12	204	0	76	12	1987	6	1987	6	1899	0	87	6	43200	3	22
50	1	50	1	49	1	1	0	1875	10	1875	10	1860	7	15	3	284	12	284	12	227	0	57	12	1997	7	1997	7	1918	0	78	7	43200	4	22
46	2	46	2	45	2	0	0	1875	10	1875	10	1856	7	19	3	272	12	272	12	209	0	63	12	1987	6	1987	6	1912	0	75	6	43200	5	22
60	2	60	2	59	2	1	0	1875	10	1875	10	1863	6	12	4	263	12	263	12	197	1	66	11	1986	7	1986	7	1909	1	76	6	43200	6	22
47	1	47	1	46	1	0	0	1875	10	1875	10	1857	7	18	3	255	11	255	11	192	0	63	11	1979	9	1979	9	1912	1	67	8	43200	7	22
48	2	48	2	48	2	0	0	1875	10	1875	10	1862	6	13	4	259	12	259	12	188	0	70	12	1967	5	1967	5	1904	0	62	5	43200	8	22
52	0	52	0	52	0	0	0	1875	10	1875	10	1856	6	19	4	275	12	275	12	207	0	68	12	1978	7	1978	7	1907	0	70	7	43200	9	22
52	1	52	1	52	1	0	0	1875	10	1875	10	1860	7	15	3	251	12	251	12	195	0	56	12	1991	6	1991	6	1919	0	71	6	43200	10	22
49	2	49	2	46	0	2	2	1875	10	1875	10	1853	6	22	4	335	12	335	12	304	0	27	12	2112	3	2112	3	1944	0	168	3	43200	1	23
58	1	58	1	57	1	0	0	1875	10	1875	10	1860	6	15	4	337	12	337	12	311	0	26	12	2120	6	2120	6	1948	0	171	6	43200	2	23
52	2	52	2	50	0	2	2	1875	10	1875	10	1857	8	18	2	352	12	352	12	316	0	22	12	2094	5	2094	5	1939	0	154	5	43200	3	23
54	0	54	0	52	0	1	0	1875	10	1875	10	1852	6	23	4	332	10	332	10	302	0	30	10	2102	8	2102	8	1945	2	157	6	43200	4	23
53	2	53	2	52	1	1	1	1875	10	1875	10	1862	8	13	2	349	10	349	10	317	2	24	8	2116	9	2116	9	1943	4	172	5	43200	5	23
48	1	48	1	48	0	0	1	1875	10	1875	10	1859	6	16	4	335	12	335	12	304	1	29	11	2116	8	2116	8	1944	1	171	7	43200	6	23
50	1	50	1	49	0	0	1	1875	10	1875	10	1853	7	22	3	372	12	358	12	306	2	37	10	2095	10	2095	10	1909	2	186	8	43200	7	23
50	2	50	2	50	0	0	2	1875	10	1875	10	1852	6	23	4	323	12	323	12	293	1	30	11	2097	7	2097	7	1945	1	151	6	43200	8	23
46	2	46	2	43	0	2	2	1875	10	1875	10	1858	6	17	4	363	12	355	12	317	1	23	11	2085	6	2085	6	1929	1	156	5	43200	9	23
53	1	53	1	50	0	2	1	1875	10	1875	10	1858	7	17	3	320	12	320	12	297	1	22	11	2099	7	2099	7	1952	1	147	6	43200	10	23
62	1	62	1	62	1	0	0	1875	10	1875	10	1866	6	9	4	485	10	358	10	275	2	68	8	1980	8	1980	8	1764	4	194	4	43200	1	24
49	2	49	2	49	2	0	0	1875	10	1875	10	1857	7	18	3	432	12	354	12	261	0	78	12	1966	7	1966	7	1803	0	161	7	43200	2	24
56	1	56	1	56	1	0	0	1875	10	1875	10	1856	6	19	4	436	11	359	11	274	3	70	8	1989	8	1989	8	1811	4	155	4	43200	3	24
45	1	45	1	45	1	0	0	1875	10	1875	10	1856	7	19	3	438	11	356	11	292	1	49	10	1976	8	1976	8	1828	2	146	6	43200	4	24
44	1	44	1	44	1	0	0	1875	10	1875	10	1856	7	19	3	481	12	345	12	278	1	52	11	1950	7	1950	7	1773	1	177	6	43200	5	24
55	1	55	1	55	1	0	0	1875	10	1875	10	1859	7	16	3	424	11	356	11	277	0	64	11	1992	9	1992	9	1827	1	163	8	43200	6	24
53	1	53	1	53	1	0	0	1875	10	1875	10	1862	6	13	4	439	12	354	12	273	0	66	12	1953	6	1953	6	1809	0	143	6	43200	7	24
58	1	58	1	58	1	0	0	1875	10	1875	10	1861	7	14	3	438	12	348	12	275	3	58	9	1952	11	1952	11	1790	3	139	8	43200	8	24
45	0	45	0	45	0	0	0	1875	10	1875	10	1854	6	21	4	475	11	344	11	275	1	54	10	1975	7	1975	7	1775	2	199	5	43200	9	24
55	1	55	1	55	1	0	0	1875	10	1875	10	1854	6	21	4	474	12	359	12	285	1	59	11	1959	6	1959	6	1786	1	172	5	43200	10	24
101	2	101	2	92	0	8	2	1875	10	1875	10	1875	10	0	0	351	10	350	10	256	1	79	9	2081	10	2081	10	1879	3	201	7	43200	1	25

101	2	101	2	90	1	10	1	1875	10	1875	10	1875	10	0	0	316	12	316	12	246	1	69	11	2084	11	2084	11	1905	1	179	10	43200	2	25
101	2	101	2	93	0	8	2	1875	10	1875	10	1875	10	0	0	327	12	327	12	253	0	74	12	2094	7	2094	7	1901	0	192	7	43200	3	25
101	2	101	2	93	0	7	2	1875	10	1875	10	1875	10	0	0	327	12	327	12	250	0	76	12	2076	10	2076	10	1898	0	178	10	43200	4	25
101	2	101	2	95	0	5	2	1875	10	1875	10	1875	10	0	0	370	12	351	12	254	3	82	9	2055	13	2055	13	1859	3	196	10	43200	5	25
101	2	101	2	96	0	4	2	1875	10	1875	10	1875	10	0	0	296	10	296	10	227	0	68	10	2071	9	2071	9	1906	2	165	7	43200	6	25
101	2	101	2	93	0	7	2	1875	10	1875	10	1875	10	0	0	320	11	320	11	242	0	75	11	2079	10	2079	10	1897	1	182	9	43200	7	25
101	2	101	2	90	0	10	2	1875	10	1875	10	1875	10	0	0	321	11	321	11	246	0	74	11	2063	10	2063	10	1900	1	163	9	43200	8	25
101	2	101	2	96	0	4	2	1875	10	1875	10	1875	10	0	0	298	12	298	12	233	1	64	11	2075	9	2075	9	1910	1	165	8	43200	9	25
101	2	101	2	93	0	7	2	1875	10	1875	10	1875	10	0	0	321	12	321	12	240	0	81	12	2076	9	2076	9	1894	0	182	9	43200	10	25
101	2	101	2	96	0	4	2	1875	10	1875	10	1875	10	0	0	454	10	347	10	326	1	6	9	1997	8	1997	8	1847	3	150	5	43200	1	26
101	2	101	2	94	0	6	2	1875	10	1875	10	1875	10	0	0	434	11	359	11	337	1	7	10	2008	9	2008	9	1878	2	130	7	43200	2	26
101	2	101	2	97	0	3	2	1875	10	1875	10	1875	10	0	0	479	12	370	12	348	0	7	12	2030	8	2030	8	1843	0	186	8	43200	3	26
101	2	101	2	97	0	3	2	1875	10	1875	10	1875	10	0	0	466	11	363	11	336	1	12	10	2001	6	2001	6	1845	2	156	4	43200	4	26
101	2	101	2	97	1	3	1	1875	10	1875	10	1875	10	0	0	465	10	365	10	344	2	6	8	2002	10	2002	10	1853	4	148	6	43200	5	26
101	2	101	2	95	0	5	2	1875	10	1875	10	1875	10	0	0	473	11	352	11	332	0	5	11	2030	7	2030	7	1833	1	196	6	43200	6	26
101	2	101	2	98	0	2	2	1875	10	1875	10	1875	10	0	0	482	11	360	11	337	1	8	10	1993	9	1993	9	1829	2	163	7	43200	7	26
101	2	101	2	95	1	5	1	1875	10	1875	10	1875	10	0	0	466	12	371	12	349	3	7	9	2018	11	2018	11	1856	3	160	8	43200	8	26
101	2	101	2	96	0	4	2	1875	10	1875	10	1875	10	0	0	475	12	360	12	330	0	15	12	1994	4	1994	4	1830	0	164	4	43200	9	26
101	2	101	2	97	0	4	2	1875	10	1875	10	1875	10	0	0	486	12	365	12	345	2	5	10	2001	11	2001	11	1834	2	166	9	43200	10	26
101	2	101	2	89	0	11	2	1875	10	1875	10	1875	10	0	0	379	11	347	11	245	0	87	11	1903	7	1903	7	1841	1	62	6	43200	1	27
101	2	101	2	97	0	3	2	1875	10	1875	10	1875	10	0	0	377	10	349	10	244	0	90	10	1897	10	1897	10	1842	2	55	8	43200	2	27
101	2	101	2	97	0	3	2	1875	10	1875	10	1875	10	0	0	340	11	340	11	243	0	93	11	1933	9	1933	9	1878	1	55	8	43200	3	27
101	2	101	2	91	0	9	2	1875	10	1875	10	1875	10	0	0	390	11	369	11	263	0	91	11	1914	10	1914	10	1848	1	66	9	43200	4	27
101	2	101	2	91	1	9	1	1875	10	1875	10	1875	10	0	0	380	12	358	12	259	0	84	12	1925	7	1925	7	1853	0	71	7	43200	5	27
101	2	101	2	97	0	3	2	1875	10	1875	10	1875	10	0	0	392	11	362	11	252	0	95	11	1905	8	1905	8	1835	1	70	7	43200	6	27
101	2	101	2	95	0	5	2	1875	10	1875	10	1875	10	0	0	368	10	365	10	243	0	107	10	1918	10	1918	10	1850	2	68	8	43200	7	27
101	2	101	2	95	0	5	2	1875	10	1875	10	1875	10	0	0	352	9	352	9	253	0	98	9	1949	8	1949	8	1876	3	73	5	43200	8	27
101	2	101	2	94	0	6	2	1875	10	1875	10	1875	10	0	0	354	12	354	12	265	0	77	12	1944	7	1944	7	1886	0	58	7	43200	9	27
101	2	101	2	94	0	6	2	1875	10	1875	10	1875	10	0	0	388	10	357	10	262	0	80	10	1913	8	1913	8	1849	2	64	6	43200	10	27
101	2	101	2	96	0	4	2	1875	10	1875	10	1875	10	0	0	230	11	230	11	211	7	19	4	2035	17	2035	17	1956	8	79	9	43200	1	28
101	2	101	2	98	0	2	2	1875	10	1875	10	1875	10	0	0	190	12	190	12	180	4	10	8	2023	13	2023	13	1965	4	58	9	43200	2	28
101	2	101	2	98	0	2	2	1875	10	1875	10	1875	10	0	0	209	12	209	12	193	4	16	8	2021	14	2021	14	1959	4	62	10	43200	3	28
101	2	101	2	97	0	3	2	1875	10	1875	10	1875	10	0	0	198	12	198	12	184	7	14	5	2019	17	2019	17	1961	7	58	10	43200	4	28
101	2	101	2	98	0	2	2	1875	10	1875	10	1875	10	0	0	219	12	219	12	201	5	18	7	2037	14	2037	14	1957	5	80	9	43200	5	28
101	2	101	2	94	0	6	2	1875	10	1875	10	1875	10	0	0	223	11	223	11	206	5	17	6	2025	14	2025	14	1958	6	67	8	43200	6	28
101	2	101	2	98	0	2	2	1875	10	1875	10	1875	10	0	0	220	11	220	11	207	3	12	8	2039	11	2039	11	1962	4	77	7	43200	7	28
101	2	101	2	97	1	3	1	1875	10	1875	10	1875	10	0	0	211	12	211	12	196	5	15	7	2033	14	2033	14	1960	5	73	9	43200	8	28
101	2	101	2	96	0	4	2	1875	10	1875	10	1875	10	0	0	222	11	222	11	212	4	10	7	2040	12	2040	12	1965	5	75	7	43200	9	28
101	2	101	2	96	0	4	2	1875	10	1875	10	1875	10	0	0	215	11	215	11	205	4	10	7	2042	12	2042	12	1965	5	77	7	43200	10	28
101	2	101	2	96	1	4	1	1875	10	1875	10	1875	10	0	0	388	7	364	7	237	1	112	6	1911	8	1911	8	1824	6	87	2	43200	1	29
101	2	101	2	99	1	1	1	1875	10	1875	10	1875	10	0	0	384	2	362	2	247	0	100	2	1922	11	1922	11	1838	10	84	1	43200	2	29
101	2	101	2	98	1	2	1	1875	10	1875	10	1875	10	0	0	432	3	368	3	247	0	106	3	1900	10	1900	10	1789	9	110	1	43200	3	29
101	2	101	2	98	1	3	1	1875	10	1875	10	1875	10	0	0	389	6	367	6	256	0	96	6	1939	9	1939	9	1843	6	96	3	43200	4	29

101	2	101	2	97	0	3	2	1875	10	1875	10	1875	10	0	0	402	6	339	6	248	0	96	6	1932	6	1932	6	1821	6	111	0	43200	5	29
101	2	101	2	96	0	4	2	1875	10	1875	10	1875	10	0	0	400	5	362	5	280	0	87	5	1934	8	1934	8	1835	7	99	1	43200	6	29
101	2	101	2	100	0	0	2	1875	10	1875	10	1875	10	0	0	425	4	367	4	236	0	116	4	1886	8	1886	8	1786	8	100	0	43200	7	29
101	2	101	2	94	0	6	2	1875	10	1875	10	1875	10	0	0	413	4	358	4	252	0	91	4	1911	9	1911	9	1814	8	97	1	43200	8	29
101	2	101	2	96	1	4	1	1875	10	1875	10	1875	10	0	0	381	5	365	5	262	0	88	5	1961	8	1961	8	1855	7	105	1	43200	9	29
101	2	101	2	97	0	3	2	1875	10	1875	10	1875	10	0	0	428	5	365	5	251	0	99	5	1912	8	1912	8	1798	7	114	1	43200	10	29
101	2	101	2	99	2	1	0	1875	10	1875	10	1875	10	0	0	245	2	245	2	224	0	21	2	2059	12	2059	12	1954	10	105	2	43200	1	30
101	2	101	2	99	2	1	0	1875	10	1875	10	1875	10	0	0	238	2	238	2	235	0	23	2	2061	10	2061	10	1952	10	109	0	43200	2	30
101	2	101	2	99	2	1	0	1875	10	1875	10	1875	10	0	0	261	3	261	3	240	0	21	3	2057	9	2057	9	1954	9	103	0	43200	3	30
101	2	101	2	100	2	0	0	1875	10	1875	10	1875	10	0	0	252	3	252	3	237	0	14	3	2066	10	2066	10	1960	9	106	1	43200	4	30
101	2	101	2	98	2	2	0	1875	10	1875	10	1875	10	0	0	279	3	279	3	267	0	11	3	2086	10	2086	10	1963	9	123	1	43200	5	30
101	2	101	2	99	2	1	0	1875	10	1875	10	1875	10	0	0	251	5	251	5	234	1	16	4	2055	8	2055	8	1958	8	97	0	43200	6	30
101	2	101	2	100	2	0	0	1875	10	1875	10	1875	10	0	0	269	1	269	1	251	1	18	0	2072	12	2072	12	1957	12	115	0	43200	7	30
101	2	101	2	99	2	1	0	1875	10	1875	10	1875	10	0	0	264	4	264	4	251	1	12	3	2088	10	2088	10	1962	9	106	1	43200	8	30
101	2	101	2	100	2	0	0	1875	10	1875	10	1875	10	0	0	268	0	268	0	244	0	24	0	2039	12	2039	12	1951	12	88	0	43200	9	30
101	2	101	2	100	2	0	0	1875	10	1875	10	1875	10	0	0	249	4	249	4	234	0	15	4	2069	10	2069	10	1960	8	109	2	43200	10	30
101	2	101	2	97	0	3	2	1875	10	1875	10	1875	10	0	0	126	3	126	3	102	0	24	3	1951	9	1951	9	1951	9	0	0	43200	1	31
101	2	101	2	95	0	5	2	1875	10	1875	10	1875	10	0	0	138	2	138	2	101	0	36	2	1938	10	1938	10	1938	10	0	0	43200	2	31
101	2	101	2	99	1	1	1	1875	10	1875	10	1875	10	0	0	118	2	118	2	94	0	24	2	1951	10	1951	10	1951	10	0	0	43200	3	31
101	2	101	2	96	0	4	2	1875	10	1875	10	1875	10	0	0	141	5	141	5	107	0	34	5	1941	7	1941	7	1941	7	0	0	43200	4	31
101	2	101	2	96	0	4	2	1875	10	1875	10	1875	10	0	0	139	4	139	4	104	0	33	4	1940	8	1940	8	1940	8	0	0	43200	5	31
101	2	101	2	95	0	5	2	1875	10	1875	10	1875	10	0	0	141	3	141	3	102	0	38	3	1936	9	1936	9	1936	9	0	0	43200	6	31
101	2	101	2	98	0	2	2	1875	10	1875	10	1875	10	0	0	117	3	117	3	97	0	20	3	1955	9	1955	9	1955	9	0	0	43200	7	31
101	2	101	2	100	0	0	2	1875	10	1875	10	1875	10	0	0	161	3	161	3	123	0	38	3	1937	9	1937	9	1937	9	0	0	43200	8	31
101	2	101	2	99	1	1	1	1875	10	1875	10	1875	10	0	0	156	3	156	3	118	0	38	3	1937	9	1937	9	1937	9	0	0	43200	9	31
101	2	101	2	98	0	2	2	1875	10	1875	10	1875	10	0	0	131	2	131	2	99	0	31	2	1943	10	1943	10	1943	10	0	0	43200	10	31
101	2	101	2	101	2	0	0	1875	10	1875	10	1875	10	0	0	292	4	292	4	292	4	0	0	1976	12	1976	12	1975	12	0	0	43200	1	32
101	2	101	2	101	2	0	0	1875	10	1875	10	1875	10	0	0	314	4	314	4	314	4	0	0	1976	12	1976	12	1975	12	0	0	43200	2	32
101	2	101	2	101	2	0	0	1875	10	1875	10	1875	10	0	0	299	2	299	2	299	2	0	0	1976	12	1976	12	1975	12	0	0	43200	3	32
101	2	101	2	101	2	0	0	1875	10	1875	10	1875	10	0	0	332	5	332	5	332	5	0	0	1976	12	1976	12	1975	12	0	0	43200	4	32
101	2	101	2	101	2	0	0	1875	10	1875	10	1875	10	0	0	282	3	282	3	282	3	0	0	1976	12	1976	12	1975	12	0	0	43200	5	32
101	2	101	2	101	2	0	0	1875	10	1875	10	1875	10	0	0	310	0	310	0	310	0	0	0	1976	12	1976	12	1975	12	0	0	43200	6	32
101	2	101	2	101	2	0	0	1875	10	1875	10	1875	10	0	0	289	1	289	1	289	1	0	0	1976	12	1976	12	1975	12	0	0	43200	7	32
101	2	101	2	101	2	0	0	1875	10	1875	10	1875	10	0	0	348	2	348	2	348	2	0	0	1976	12	1976	12	1975	12	0	0	43200	8	32
101	2	101	2	101	2	0	0	1875	10	1875	10	1875	10	0	0	294	3	294	3	294	3	0	0	1976	12	1976	12	1975	12	0	0	43200	9	32
101	2	101	2	101	2	0	0	1875	10	1875	10	1875	10	0	0	319	3	319	3	319	3	0	0	1976	12	1976	12	1975	12	0	0	43200	10	32
82	0	82	0	82	0	0	0	1875	10	1875	10	1875	10	0	0	338	12	352	12	251	0	88	10	2020	12	2020	12	1868	0	151	12	43200	1	33
76	2	76	2	76	2	0	0	1875	10	1875	10	1875	10	0	0	371	11	351	10	232	0	104	10	1990	8	1990	8	1837	1	153	7	43200	2	33
80	0	80	0	80	0	0	0	1875	10	1875	10	1875	10	0	0	366	10	363	10	259	1	90	8	2040	13	2040	13	1868	3	171	10	43200	3	33
77	1	77	1	77	1	0	0	1875	10	1875	10	1875	10	0	0	392	11	345	9	238	0	92	9	1987	12	1987	12	1821	1	165	11	43200	4	33
82	2	82	2	82	2	0	0	1875	10	1875	10	1875	10	0	0	357	12	350	12	244	0	93	10	2014	11	2014	11	1862	0	151	11	43200	5	33
77	2	77	2	77	2	0	0	1875	10	1875	10	1875	10	0	0	406	11	365	11	280	2	90	9	2004	12	2004	12	1829	3	174	9	43200	6	33
66	1	66	1	66	1	0	0	1875	10	1875	10	1875	10	0	0	412	11	350	10	237	0	98	10	1981	8	1981	8	1799	1	180	7	43200	7	33

74	2	74	2	74	2	0	0	1875	10	1875	10	1875	10	0	0	392	12	335	11	238	0	102	11	1995	7	1995	7	1821	0	173	7	43200	8	33
76	1	76	1	76	1	0	0	1875	10	1875	10	1875	10	0	0	422	12	349	10	236	0	98	10	1971	12	1971	12	1789	0	181	12	43200	9	33
71	2	71	2	71	2	0	0	1875	10	1875	10	1875	10	0	0	438	11	357	10	255	0	87	10	1976	9	1976	9	1792	1	183	8	43200	10	33
18	1	18	1	18	1	0	0	1875	10	1875	10	1875	10	0	0	305	11	305	11	211	0	94	11	2073	11	2073	11	1881	1	191	10	43200	1	34
31	2	31	2	30	2	1	0	1875	10	1875	10	1875	10	0	0	293	12	293	12	211	0	81	12	2070	12	2070	12	1893	0	176	12	43200	2	34
20	1	20	1	19	1	1	0	1875	10	1875	10	1875	10	0	0	312	12	312	12	227	0	84	12	2096	12	2096	12	1890	0	205	12	43200	3	34
30	1	30	1	28	1	2	0	1875	10	1875	10	1875	10	0	0	287	12	287	12	212	0	74	12	2077	10	2077	10	1900	0	176	10	43200	4	34
19	1	19	1	18	1	1	0	1875	10	1875	10	1875	10	0	0	292	10	292	10	218	0	72	10	2072	11	2072	11	1901	2	170	9	43200	5	34
29	1	29	1	25	1	4	0	1875	10	1875	10	1875	10	0	0	304	12	304	12	206	0	98	12	2053	12	2053	12	1877	0	175	12	43200	6	34
33	0	33	0	32	0	0	0	1875	10	1875	10	1875	10	0	0	305	11	305	11	212	0	93	11	2062	12	2062	12	1882	1	180	11	43200	7	34
26	0	26	0	25	0	1	0	1875	10	1875	10	1875	10	0	0	280	11	280	11	208	0	71	11	2080	11	2080	11	1904	1	176	10	43200	8	34
32	0	32	0	31	0	1	0	1875	10	1875	10	1875	10	0	0	280	11	280	11	191	0	89	11	2053	12	2053	12	1886	1	166	11	43200	9	34
20	0	20	0	18	0	1	0	1875	10	1875	10	1875	10	0	0	270	11	270	11	184	0	84	11	2042	12	2042	12	1889	1	153	11	43200	10	34
22	1	22	1	19	0	2	1	1875	10	1875	10	1875	10	0	0	247	10	247	10	235	7	12	3	2112	18	2112	18	1963	9	149	9	43200	1	35
24	1	24	1	22	0	1	1	1875	10	1875	10	1875	10	0	0	288	9	288	9	265	7	22	2	2131	18	2131	18	1952	10	179	8	43200	2	35
26	0	26	0	25	0	1	0	1875	10	1875	10	1875	10	0	0	305	10	305	10	289	7	15	3	2147	17	2147	17	1959	9	187	8	43200	3	35
33	0	33	0	30	0	2	0	1875	10	1875	10	1875	10	0	0	270	12	270	12	255	9	13	3	2135	20	2135	20	1980	9	175	11	43200	4	35
25	1	25	1	24	0	0	1	1875	10	1875	10	1875	10	0	0	282	12	282	12	277	8	5	4	2150	19	2150	19	1970	8	180	11	43200	5	35
25	0	25	0	22	0	3	0	1875	10	1875	10	1875	10	0	0	257	12	257	12	241	10	15	2	2118	20	2118	20	1959	10	158	10	43200	6	35
29	1	29	1	29	0	0	1	1875	10	1875	10	1875	10	0	0	278	11	278	11	264	7	14	4	2141	17	2141	17	1961	8	179	9	43200	7	35
27	0	27	0	24	0	3	0	1875	10	1875	10	1875	10	0	0	302	12	302	12	288	9	13	3	2161	20	2161	20	1961	9	199	11	43200	8	35
26	1	26	1	22	0	4	1	1875	10	1875	10	1875	10	0	0	273	11	273	11	255	7	16	4	2127	18	2127	18	1957	8	169	10	43200	9	35
22	2	22	2	20	0	2	2	1875	10	1875	10	1875	10	0	0	287	12	287	12	275	8	12	4	2128	17	2128	17	1963	8	164	9	43200	10	35
20	0	20	0	19	0	1	0	1875	10	1875	10	1875	10	0	0	149	11	149	11	120	1	29	10	2025	13	2025	13	1946	2	78	11	43200	1	36
28	2	28	2	27	2	1	0	1875	10	1875	10	1875	10	0	0	148	12	148	12	116	1	32	11	2026	13	2026	13	1943	1	82	12	43200	2	36
17	1	17	1	15	1	2	0	1875	10	1875	10	1875	10	0	0	135	12	135	12	108	0	27	12	2019	12	2019	12	1948	0	70	12	43200	3	36
22	0	22	0	22	0	0	0	1875	10	1875	10	1875	10	0	0	132	10	132	10	94	0	36	10	2001	12	2001	12	1937	2	63	10	43200	4	36
23	1	23	1	20	1	2	0	1875	10	1875	10	1875	10	0	0	168	10	168	10	123	0	45	10	2007	12	2007	12	1930	2	77	10	43200	5	36
27	1	27	1	26	0	1	1	1875	10	1875	10	1875	10	0	0	151	11	151	11	128	0	22	11	2014	10	2014	10	1952	1	61	9	43200	6	36
25	0	25	0	23	0	2	0	1875	10	1875	10	1875	10	0	0	176	10	176	10	122	0	53	10	2004	12	2004	12	1921	2	82	10	43200	7	36
25	0	25	0	23	0	2	0	1875	10	1875	10	1875	10	0	0	162	11	162	11	125	1	36	10	2026	13	2026	13	1938	2	87	11	43200	8	36
23	1	23	1	22	1	1	0	1875	10	1875	10	1875	10	0	0	156	11	156	11	124	0	31	11	2021	12	2021	12	1943	1	77	11	43200	9	36
23	1	23	1	23	1	0	0	1875	10	1875	10	1875	10	0	0	157	12	157	12	122	0	35	12	2010	10	2010	10	1940	0	69	10	43200	10	36
26	0	26	0	24	0	2	0	1875	10	1875	10	1875	10	0	0	198	9	198	9	194	1	4	8	2036	11	2036	11	1971	4	64	7	43200	1	37
22	1	22	1	20	0	2	1	1875	10	1875	10	1875	10	0	0	207	11	207	11	204	2	3	9	2052	13	2052	13	1972	3	79	10	43200	2	37
21	0	21	0	20	0	1	0	1875	10	1875	10	1875	10	0	0	216	10	216	10	210	0	6	10	2037	12	2037	12	1969	2	67	10	43200	3	37
28	1	28	1	27	1	1	0	1875	10	1875	10	1875	10	0	0	211	12	211	12	206	2	4	10	2044	13	2044	13	1970	2	73	11	43200	4	37
31	0	31	0	28	0	3	0	1875	10	1875	10	1875	10	0	0	220	11	220	11	215	3	4	8	2052	13	2052	13	1970	4	81	9	43200	5	37
27	0	27	0	24	0	3	0	1875	10	1875	10	1875	10	0	0	211	11	211	11	209	2	2	9	2043	14	2043	14	1973	3	69	11	43200	6	37
22	0	22	0	18	0	4	0	1875	10	1875	10	1875	10	0	0	223	11	223	11	217	3	5	8	2055	15	2055	15	1969	4	83	11	43200	7	37
24	1	24	1	21	0	2	1	1875	10	1875	10	1875	10	0	0	232	10	232	10	226	2	6	8	2048	12	2048	12	1969	4	79	8	43200	8	37
29	0	29	0	26	0	2	0	1875	10	1875	10	1875	10	0	0	212	10	212	10	209	3	3	7	2046	14	2046	14	1972	5	74	9	43200	9	37
23	0	23	0	18	0	5	0	1875	10	1875	10	1875	10	0	0	213	11	213	11	211	4	1	7	2051	15	2051	15	1974	5	77	10	43200	10	37

27	1	27	1	24	0	3	1	1875	10	1875	10	1875	10	0	0	337	3	337	3	258	0	79	3	1996	9	1996	9	1896	9	99	0	43200	1	38
30	0	30	0	26	0	3	0	1875	10	1875	10	1875	10	0	0	336	6	336	6	258	0	78	6	2010	7	2010	7	1897	6	113	1	43200	2	38
24	0	24	0	21	0	3	0	1875	10	1875	10	1875	10	0	0	297	0	297	0	223	0	73	0	2004	12	2004	12	1901	12	102	0	43200	3	38
30	0	30	0	24	0	6	0	1875	10	1875	10	1875	10	0	0	327	1	327	1	237	0	90	1	1998	11	1998	11	1885	11	112	0	43200	4	38
20	1	20	1	18	0	2	1	1875	10	1875	10	1875	10	0	0	313	6	313	6	234	0	79	6	1982	7	1982	7	1896	6	85	1	43200	5	38
28	1	28	1	26	0	1	1	1875	10	1875	10	1875	10	0	0	289	5	289	5	223	0	66	5	2002	9	2002	9	1909	7	93	2	43200	6	38
28	2	28	2	24	1	4	1	1875	10	1875	10	1875	10	0	0	316	5	316	5	249	0	67	5	2010	8	2010	8	1908	7	101	1	43200	7	38
24	1	24	1	23	0	1	1	1875	10	1875	10	1875	10	0	0	296	5	296	5	218	0	77	5	2001	8	2001	8	1897	7	103	1	43200	8	38
20	1	20	1	18	0	2	1	1875	10	1875	10	1875	10	0	0	323	3	323	3	261	0	62	3	2034	10	2034	10	1913	9	120	1	43200	9	38
23	1	23	1	19	0	4	1	1875	10	1875	10	1875	10	0	0	287	7	287	7	218	0	68	7	2003	8	2003	8	1906	5	96	3	43200	10	38
26	1	26	1	24	0	2	1	1875	10	1875	10	1875	10	0	0	337	3	337	3	335	2	2	1	2079	12	2079	12	1973	11	105	1	43200	1	39
24	1	24	1	21	0	2	1	1875	10	1875	10	1875	10	0	0	325	5	325	5	323	4	2	1	2071	13	2071	13	1973	11	98	2	43200	2	39
21	1	21	1	19	0	2	1	1875	10	1875	10	1875	10	0	0	337	7	337	7	332	5	3	2	2072	13	2072	13	1970	10	101	3	43200	3	39
18	1	18	1	15	0	3	1	1875	10	1875	10	1875	10	0	0	325	7	325	7	316	5	8	2	2056	11	2056	11	1966	10	89	1	43200	4	39
17	0	17	0	13	0	3	0	1875	10	1875	10	1875	10	0	0	332	4	332	4	330	2	1	2	2063	13	2063	13	1973	10	90	3	43200	5	39
21	0	21	0	19	0	2	0	1875	10	1875	10	1875	10	0	0	327	3	327	3	323	2	2	1	2080	12	2080	12	1972	11	88	1	43200	6	39
23	0	23	0	22	0	1	0	1875	10	1875	10	1875	10	0	0	353	2	353	2	348	2	4	0	2077	14	2077	14	1969	12	106	2	43200	7	39
21	1	21	1	18	0	3	1	1875	10	1875	10	1875	10	0	0	376	3	370	3	354	2	1	1	2058	12	2058	12	1953	11	104	1	43200	8	39
39	0	39	0	36	0	3	0	1875	10	1875	10	1875	10	0	0	335	2	335	2	332	2	3	0	2074	13	2074	13	1972	12	101	1	43200	9	39
24	0	24	0	20	0	3	0	1875	10	1875	10	1875	10	0	0	380	5	367	5	352	3	0	2	2053	11	2053	11	1947	10	106	1	43200	10	39
34	2	34	2	30	0	4	2	1875	10	1875	10	1875	10	0	0	228	5	228	5	170	1	58	4	1918	8	1918	8	1917	8	0	0	43200	1	40
21	0	21	0	21	0	0	0	1875	10	1875	10	1875	10	0	0	230	2	230	2	155	0	74	2	1901	10	1901	10	1900	10	0	0	43200	2	40
18	1	18	1	15	0	2	1	1875	10	1875	10	1875	10	0	0	223	4	223	4	161	0	62	4	1913	8	1913	8	1913	8	0	0	43200	3	40
26	1	26	1	22	0	4	1	1875	10	1875	10	1875	10	0	0	258	5	258	5	178	0	76	5	1896	7	1896	7	1896	7	0	0	43200	4	40
25	2	25	2	25	0	0	2	1875	10	1875	10	1875	10	0	0	219	4	219	4	158	0	60	4	1915	8	1915	8	1914	8	0	0	43200	5	40
29	0	29	0	28	0	1	0	1875	10	1875	10	1875	10	0	0	236	4	236	4	161	0	75	4	1901	8	1901	8	1900	8	0	0	43200	6	40
21	0	21	0	19	0	2	0	1875	10	1875	10	1875	10	0	0	247	1	247	1	175	0	70	1	1904	11	1904	11	1903	11	0	0	43200	7	40
17	0	17	0	16	0	1	0	1875	10	1875	10	1875	10	0	0	258	6	258	6	199	0	59	6	1917	6	1917	6	1916	6	0	0	43200	8	40
27	1	27	1	22	0	4	1	1875	10	1875	10	1875	10	0	0	224	2	224	2	169	0	54	2	1920	10	1920	10	1920	10	0	0	43200	9	40
18	1	18	1	15	0	3	1	1875	10	1875	10	1875	10	0	0	235	2	235	2	181	0	54	2	1922	10	1922	10	1921	10	0	0	43200	10	40
28	0	28	0	22	0	6	0	1875	10	1875	10	1875	10	0	0	221	3	221	3	208	0	13	3	1963	9	1963	9	1962	9	0	0	43200	1	41
25	0	25	0	18	0	7	0	1875	10	1875	10	1875	10	0	0	219	3	219	3	202	0	17	3	1959	9	1959	9	1958	9	0	0	43200	2	41
22	1	22	1	21	0	1	1	1875	10	1875	10	1875	10	0	0	237	2	237	2	217	0	18	2	1956	10	1956	10	1955	10	0	0	43200	3	41
28	1	28	1	21	0	6	1	1875	10	1875	10	1875	10	0	0	236	4	236	4	216	0	19	4	1955	8	1955	8	1955	8	0	0	43200	4	41
19	0	19	0	16	0	3	0	1875	10	1875	10	1875	10	0	0	192	1	192	1	170	0	21	1	1954	11	1954	11	1954	11	0	0	43200	5	41
28	0	28	0	26	0	2	0	1875	10	1875	10	1875	10	0	0	205	3	205	3	191	0	14	3	1962	9	1962	9	1961	9	0	0	43200	6	41
26	0	26	0	25	0	1	0	1875	10	1875	10	1875	10	0	0	203	3	203	3	187	0	16	3	1980	9	1980	9	1959	9	0	0	43200	7	41
27	0	27	0	25	0	2	0	1875	10	1875	10	1875	10	0	0	228	4	228	4	211	0	16	4	1959	8	1959	8	1958	8	0	0	43200	8	41
32	1	32	1	29	0	3	1	1875	10	1875	10	1875	10	0	0	195	3	195	3	181	0	14	3	1962	9	1962	9	1961	9	0	0	43200	9	41
19	0	19	0	17	0	2	0	1875	10	1875	10	1875	10	0	0	217	4	217	4	194	0	22	4	1953	8	1953	8	1952	8	0	0	43200	10	41
101	2	101	2	95	2	5	0	1875	10	1875	10	1880	6	15	4	193	4	193	4	168	0	25	4	1951	8	1951	8	1950	8	1	0	43200	1	42
101	2	101	2	88	2	12	0	1875	10	1875	10	1852	6	23	4	188	4	188	4	170	0	18	4	1958	8	1958	8	1957	8	1	0	43200	2	42
101	2	101	2	94	2	6	0	1875	10	1875	10	1890	6	25	4	193	4	193	4	170	1	23	3	1955	9	1955	9	1951	9	3	0	43200	3	42

101	2	101	2	94	2	6	0	1875	10	1875	10	1849	6	26	4	198	4	198	4	174	0	23	4	1933	8	1933	8	1951	8	2	0	43200	4	42
101	2	101	2	94	2	6	0	1875	10	1875	10	1851	7	24	3	189	4	189	4	166	1	22	3	1955	9	1955	9	1952	9	3	0	43200	5	42
101	2	101	2	97	2	3	0	1875	10	1875	10	1855	6	20	4	163	4	163	4	142	0	21	4	1955	8	1955	8	1954	8	1	0	43200	6	42
101	2	101	2	94	2	6	0	1875	10	1875	10	1862	6	13	4	190	5	190	5	157	0	33	5	1943	7	1943	7	1942	7	1	0	43200	7	42
101	2	101	2	91	2	9	0	1875	10	1875	10	1857	6	18	4	188	4	188	4	167	0	21	4	1955	8	1955	8	1954	8	1	0	43200	8	42
101	2	101	2	92	2	8	0	1875	10	1875	10	1859	6	16	4	158	4	158	4	136	0	22	4	1954	8	1954	8	1953	8	1	0	43200	9	42
101	2	101	2	93	2	7	0	1875	10	1875	10	1859	6	16	4	169	6	169	6	148	1	21	5	1957	7	1957	7	1954	7	3	0	43200	10	42
101	2	101	2	90	0	10	2	1875	10	1875	10	1863	6	12	4	120	6	120	6	94	0	24	6	1950	6	1950	6	1949	6	1	0	43200	1	43
101	2	101	2	89	0	11	2	1875	10	1875	10	1857	6	18	4	92	7	92	7	68	0	23	7	1952	5	1952	5	1951	5	1	0	43200	2	43
101	2	101	2	92	0	8	2	1875	10	1875	10	1854	6	21	4	93	6	93	6	74	0	19	6	1957	6	1957	6	1956	6	1	0	43200	3	43
101	2	101	2	93	1	7	1	1875	10	1875	10	1859	5	16	5	107	6	107	6	85	0	22	6	1954	6	1954	6	1953	6	1	0	43200	4	43
101	2	101	2	93	0	7	2	1875	10	1875	10	1861	6	14	4	86	6	86	6	59	0	25	6	1949	6	1949	6	1948	6	1	0	43200	5	43
101	2	101	2	94	0	6	2	1875	10	1875	10	1862	6	13	4	102	6	102	6	71	0	30	6	1945	6	1945	6	1944	6	1	0	43200	6	43
101	2	101	2	96	0	4	2	1875	10	1875	10	1854	6	21	4	100	6	100	6	77	1	23	5	1955	7	1955	7	1952	7	3	0	43200	7	43
101	2	101	2	93	1	7	1	1875	10	1875	10	1854	6	21	4	104	5	104	5	83	0	20	5	1957	7	1957	7	1954	7	3	0	43200	8	43
101	2	101	2	92	0	8	2	1875	10	1875	10	1862	6	13	4	91	7	91	7	74	1	16	6	1959	6	1959	6	1958	6	1	0	43200	9	43
101	2	101	2	90	0	10	2	1875	10	1875	10	1858	6	17	4	103	6	103	6	76	0	26	6	1949	6	1949	6	1948	6	1	0	43200	10	43
101	2	101	2	89	2	11	0	1875	10	1875	10	1853	7	22	3	200	5	200	5	195	2	5	3	2080	10	2080	10	1970	9	110	1	43200	1	44
101	2	101	2	88	2	12	0	1875	10	1875	10	1857	6	18	4	165	6	165	6	152	2	13	4	2048	8	2048	8	1962	8	86	0	43200	2	44
101	2	101	2	94	2	6	0	1875	10	1875	10	1847	6	28	4	194	4	194	4	183	1	11	3	2071	9	2071	9	1964	9	107	0	43200	3	44
101	2	101	2	88	2	12	0	1875	10	1875	10	1850	6	25	4	199	4	199	4	192	1	6	3	2068	9	2068	9	1968	9	100	0	43200	4	44
101	2	101	2	95	2	5	0	1875	10	1875	10	1859	7	16	3	197	3	197	3	183	0	12	3	2078	9	2078	9	1961	9	117	0	43200	5	44
101	2	101	2	89	2	11	0	1875	10	1875	10	1853	6	22	4	175	5	175	5	167	2	8	3	2050	10	2050	10	1967	9	83	1	43200	6	44
101	2	101	2	90	2	10	0	1875	10	1875	10	1860	6	15	4	178	4	178	4	168	0	10	4	2063	8	2063	8	1965	8	98	0	43200	7	44
101	2	101	2	93	2	7	0	1875	10	1875	10	1862	8	13	2	193	3	193	3	177	0	15	3	2070	9	2070	9	1959	9	111	0	43200	8	44
101	2	101	2	92	2	8	0	1875	10	1875	10	1862	6	13	4	192	4	192	4	178	0	13	4	2066	8	2066	8	1961	8	105	0	43200	9	44
101	2	101	2	93	2	7	0	1875	10	1875	10	1857	7	18	3	178	6	178	6	166	2	11	4	2052	10	2052	10	1963	8	89	2	43200	10	44
101	2	101	2	94	0	7	2	1875	10	1875	10	1856	6	19	4	289	7	289	7	232	1	57	6	2020	7	2020	7	1918	6	101	1	43200	1	45
101	2	101	2	91	0	9	2	1875	10	1875	10	1862	6	13	4	293	8	293	8	239	0	52	8	2035	6	2035	6	1921	4	114	2	43200	2	45
101	2	101	2	90	0	11	2	1875	10	1875	10	1853	6	22	4	281	7	281	7	218	0	62	7	2009	5	2009	5	1912	5	96	0	43200	3	45
101	2	101	2	88	1	12	1	1875	10	1875	10	1854	6	21	4	300	5	300	5	229	0	70	5	2004	7	2004	7	1904	7	100	0	43200	4	45
101	2	101	2	89	0	11	2	1875	10	1875	10	1853	7	22	3	272	6	272	6	219	0	53	6	2005	6	2005	6	1922	6	83	0	43200	5	45
101	2	101	2	90	0	10	2	1875	10	1875	10	1860	6	15	4	281	7	281	7	232	0	49	7	2028	5	2028	5	1926	5	102	0	43200	6	45
101	2	101	2	93	0	7	2	1875	10	1875	10	1847	5	28	5	280	7	280	7	234	0	46	7	2038	5	2038	5	1929	5	109	0	43200	7	45
101	2	101	2	89	0	11	2	1875	10	1875	10	1864	6	11	4	290	6	290	6	233	1	56	5	2028	7	2028	7	1918	7	110	0	43200	8	45
101	2	101	2	89	0	11	2	1875	10	1875	10	1856	6	19	4	286	6	286	6	229	1	56	5	2013	7	2013	7	1918	7	95	0	43200	9	45
101	2	101	2	89	0	11	2	1875	10	1875	10	1857	6	18	4	291	10	291	10	232	1	59	9	2014	6	2014	6	1916	3	98	3	43200	10	45
101	2	101	2	94	0	6	2	1875	10	1875	10	1862	8	13	2	299	12	299	12	282	1	16	11	2040	6	2040	6	1958	1	82	5	43200	1	46
101	2	101	2	86	0	14	2	1875	10	1875	10	1851	6	24	4	307	12	307	12	295	2	12	10	2031	7	2031	7	1962	2	68	5	43200	2	46
101	2	101	2	87	0	13	2	1875	10	1875	10	1853	7	22	3	294	11	294	11	267	0	27	11	2019	6	2019	6	1948	1	71	5	43200	3	46
101	2	101	2	93	0	7	2	1875	10	1875	10	1849	8	26	2	295	11	295	11	283	1	12	10	2032	7	2032	7	1963	2	69	5	43200	4	46
101	2	101	2	87	0	13	2	1875	10	1875	10	1857	6	18	4	298	12	298	12	282	3	15	9	2036	8	2036	8	1959	3	77	5	43200	5	46
101	2	101	2	91	0	9	2	1875	10	1875	10	1856	6	19	4	288	12	288	12	265	0	21	12	2019	5	2019	5	1952	0	67	5	43200	6	46

101	2	101	2	91	0	9	2	1875	10	1875	10	1844	6	31	4	298	12	298	12	272	4	24	8	2012	8	2012	8	1949	4	63	4	43200	7	46
101	2	101	2	86	0	14	2	1875	10	1875	10	1851	6	24	4	324	12	324	12	291	1	30	11	2025	5	2025	5	1942	1	83	4	43200	8	46
101	2	101	2	93	0	7	2	1875	10	1875	10	1856	6	19	4	295	11	295	11	276	3	18	8	2036	7	2036	7	1956	4	80	3	43200	9	46
101	2	101	2	93	0	7	2	1875	10	1875	10	1853	6	22	4	291	11	291	11	276	1	12	10	2029	6	2029	6	1980	2	69	4	43200	10	46
101	2	101	2	94	0	7	2	1875	10	1875	10	1858	6	17	4	342	12	342	12	284	0	57	12	1984	6	1984	6	1917	0	66	6	43200	1	47
101	2	101	2	86	0	14	2	1875	10	1875	10	1859	6	16	4	338	12	344	12	264	1	65	11	1953	5	1953	5	1881	1	72	4	43200	2	47
101	2	101	2	87	0	13	2	1875	10	1875	10	1860	6	15	4	339	11	339	11	264	0	72	11	1980	4	1980	4	1900	1	60	3	43200	3	47
101	2	101	2	92	0	9	2	1875	10	1875	10	1862	6	13	4	344	12	344	12	278	0	63	12	1975	5	1975	5	1909	0	65	5	43200	4	47
101	2	101	2	87	0	13	2	1875	10	1875	10	1852	9	23	1	355	11	355	11	285	1	60	10	1985	7	1985	7	1904	2	80	5	43200	5	47
101	2	101	2	87	0	13	2	1875	10	1875	10	1858	6	17	4	353	12	352	12	270	2	67	10	1961	6	1961	6	1891	2	69	4	43200	6	47
101	2	101	2	85	0	15	2	1875	10	1875	10	1851	6	24	4	348	10	348	10	283	1	64	9	1973	6	1973	6	1910	3	63	3	43200	7	47
101	2	101	2	91	0	9	2	1875	10	1875	10	1856	6	19	4	313	12	313	12	266	0	47	12	1998	4	1998	4	1928	0	70	4	43200	8	47
101	2	101	2	88	1	12	1	1875	10	1875	10	1853	6	22	4	332	12	332	12	263	1	66	11	1964	6	1964	6	1906	1	58	5	43200	9	47
101	2	101	2	85	0	15	2	1875	10	1875	10	1860	7	15	3	338	12	338	12	271	1	66	11	1977	7	1977	7	1908	1	69	6	43200	10	47
101	2	101	2	94	0	6	2	1875	10	1875	10	1851	6	20	4	343	12	339	12	308	4	34	8	2015	7	2015	7	1851	4	164	3	43200	1	48
101	2	101	2	88	0	12	2	1875	10	1875	10	1856	6	19	4	443	12	355	12	304	3	36	9	1992	6	1992	6	1836	3	156	3	43200	2	48
101	2	101	2	90	0	10	2	1875	10	1875	10	1860	6	15	4	433	12	346	12	295	8	36	4	1996	13	1996	13	1836	8	139	5	43200	3	48
101	2	101	2	94	1	6	1	1875	10	1875	10	1855	6	20	4	397	12	355	12	310	5	30	7	2037	11	2037	11	1887	5	149	6	43200	4	48
101	2	101	2	90	1	10	1	1875	10	1875	10	1859	6	16	4	433	12	359	12	308	7	36	5	2012	12	2012	12	1849	7	162	5	43200	5	48
101	2	101	2	93	0	7	2	1875	10	1875	10	1860	6	15	4	455	11	348	11	304	5	29	6	1993	10	1993	10	1824	6	169	4	43200	6	48
101	2	101	2	83	0	17	2	1875	10	1875	10	1853	6	22	4	424	12	360	12	310	4	35	8	2024	10	2024	10	1861	4	163	6	43200	7	48
101	2	101	2	95	0	5	2	1875	10	1875	10	1851	7	24	3	430	10	350	10	297	6	38	4	2013	13	2013	13	1841	8	171	5	43200	8	48
101	2	101	2	87	1	13	1	1875	10	1875	10	1854	6	21	4	463	12	354	12	303	8	36	4	1977	12	1977	12	1814	8	162	4	43200	9	48
101	2	101	2	88	0	12	2	1875	10	1875	10	1855	6	20	4	431	10	356	10	302	5	39	5	2008	10	2008	10	1846	7	162	3	43200	10	48
101	2	101	2	92	0	8	2	1875	10	1875	10	1854	7	21	3	382	10	355	10	280	0	80	10	2021	7	2021	7	1853	2	168	5	43200	1	49
101	2	101	2	84	0	16	2	1875	10	1875	10	1863	6	12	4	380	12	364	12	266	1	83	11	2030	6	2030	6	1861	1	169	5	43200	2	49
101	2	101	2	88	0	12	2	1875	10	1875	10	1857	6	18	4	372	12	361	12	280	0	86	12	2010	3	2010	3	1863	0	147	3	43200	3	49
101	2	101	2	91	0	9	2	1875	10	1875	10	1858	6	17	4	392	12	348	12	251	0	82	12	2022	5	2022	5	1833	0	188	5	43200	4	49
101	2	101	2	89	0	11	2	1875	10	1875	10	1849	7	26	3	379	12	349	12	239	0	75	12	2018	5	2018	5	1855	0	163	5	43200	5	49
101	2	101	2	92	0	8	2	1875	10	1875	10	1854	6	21	4	414	12	362	12	268	0	79	12	2014	4	2014	4	1829	0	185	4	43200	6	49
101	2	101	2	89	0	11	2	1875	10	1875	10	1856	7	19	3	362	12	358	12	262	0	81	12	2041	6	2041	6	1874	0	166	6	43200	7	49
101	2	101	2	84	0	16	2	1875	10	1875	10	1860	6	15	4	393	12	355	12	231	1	109	11	1994	4	1994	4	1813	1	181	3	43200	8	49
101	2	101	2	82	0	18	2	1875	10	1875	10	1851	6	24	4	406	12	359	12	264	0	80	12	1992	5	1992	5	1833	0	139	5	43200	9	49
101	2	101	2	86	0	14	2	1875	10	1875	10	1851	6	24	4	385	12	356	12	247	0	94	12	2005	5	2005	5	1836	0	168	5	43200	10	49
80	2	80	2	77	2	3	0	1875	10	1875	10	1803	1	72	9	475	12	348	12	251	0	82	12	1881	3	1881	3	1751	0	129	3	43200	1	50
80	2	80	2	76	2	4	0	1875	10	1875	10	1810	0	65	10	490	12	351	12	262	0	74	12	1906	1	1906	1	1747	0	138	1	43200	2	50
80	2	80	2	76	2	3	0	1875	10	1875	10	1796	1	79	9	501	12	358	12	267	0	76	12	1895	2	1895	2	1740	0	154	2	43200	3	50
88	2	88	2	85	2	2	0	1875	10	1875	10	1783	1	92	9	522	12	345	12	230	0	80	12	1866	2	1866	2	1703	0	163	2	43200	4	50
79	2	79	2	71	2	7	0	1875	10	1875	10	1812	2	63	8	499	12	357	12	239	0	83	12	1882	2	1882	2	1734	0	147	2	43200	5	50
78	2	78	2	73	2	5	0	1875	10	1875	10	1808	2	67	8	504	12	364	12	238	0	91	12	1887	3	1887	3	1729	0	157	3	43200	6	50
73	1	73	1	68	1	4	0	1875	10	1875	10	1796	1	79	9	501	11	353	11	264	0	74	11	1877	2	1877	2	1737	1	139	1	43200	7	50
78	2	78	2	73	2	5	0	1875	10	1875	10	1801	1	74	9	518	12	363	12	235	0	93	12	1865	3	1865	3	1712	0	152	3	43200	8	50
86	2	86	2	81	2	4	0	1875	10	1875	10	1800	0	75	10	516	11	352	11	269	0	68	11	1885	1	1885	1	1726	1	157	0	43200	9	50

81	2	81	2	75	2	5	0	1875	10	1875	10	1803	3	72	7	465	12	338	12	252	0	91	12	1897	4	1897	4	1780	0	135	4	43200	10	50
78	2	78	2	73	1	4	1	1875	10	1875	10	1802	1	73	9	414	12	363	12	315	4	33	8	2061	6	2061	6	1874	4	185	2	43200	1	51
80	2	80	2	74	1	5	1	1875	10	1875	10	1802	0	73	10	380	12	368	12	320	8	33	4	2077	8	2077	8	1915	8	162	0	43200	2	51
80	1	80	1	74	0	5	1	1875	10	1875	10	1802	1	73	9	390	12	367	12	328	8	24	4	2079	9	2079	9	1913	8	166	1	43200	3	51
70	0	70	0	61	0	8	0	1875	10	1875	10	1797	3	78	7	403	12	366	12	323	6	28	6	2043	10	2043	10	1895	6	148	4	43200	4	51
74	1	74	1	66	0	7	1	1875	10	1875	10	1782	1	93	9	417	12	352	12	311	5	26	7	2017	7	2017	7	1869	5	148	2	43200	5	51
82	2	82	2	76	0	5	2	1875	10	1875	10	1794	0	81	10	389	12	352	12	307	5	30	7	2042	5	2042	5	1893	5	149	0	43200	6	51
75	0	75	0	68	0	6	0	1875	10	1875	10	1801	0	74	10	392	12	362	12	312	5	35	7	2062	6	2062	6	1895	5	167	1	43200	7	51
77	1	77	1	71	0	5	1	1875	10	1875	10	1799	2	76	8	396	11	330	11	300	5	35	6	2030	7	2030	7	1878	6	171	1	43200	8	51
75	2	75	2	71	0	3	2	1875	10	1875	10	1807	0	68	10	401	12	362	12	317	4	30	8	2089	4	2089	4	1890	4	178	0	43200	9	51
74	2	74	2	71	0	2	2	1875	10	1875	10	1792	0	83	10	413	12	352	12	310	7	27	5	2046	7	2046	7	1871	7	174	0	43200	10	51
82	1	82	1	72	1	9	0	1875	10	1875	10	1817	0	58	10	278	12	278	12	227	1	51	11	1999	3	1999	3	1924	1	75	2	43200	1	52
72	2	72	2	68	1	3	1	1875	10	1875	10	1801	2	74	8	291	12	291	12	231	0	59	12	1985	2	1985	2	1915	0	70	2	43200	2	52
77	1	77	1	71	1	5	0	1875	10	1875	10	1815	1	60	9	293	11	293	11	239	1	53	10	1994	4	1994	4	1921	2	73	2	43200	3	52
70	2	70	2	69	1	1	1	1875	10	1875	10	1802	0	73	10	306	12	306	12	249	2	56	10	1994	3	1994	3	1918	2	75	1	43200	4	52
76	1	76	1	69	1	7	0	1875	10	1875	10	1794	1	81	9	302	11	302	11	245	0	55	11	1994	1	1994	1	1919	1	75	0	43200	5	52
82	1	82	1	75	1	6	0	1875	10	1875	10	1798	0	77	10	286	12	286	12	236	3	49	9	1991	5	1991	5	1925	3	66	2	43200	6	52
77	2	77	2	70	2	6	0	1875	10	1875	10	1803	0	72	10	321	12	321	12	252	0	67	12	1981	2	1981	2	1906	0	75	2	43200	7	52
81	1	81	1	74	1	6	0	1875	10	1875	10	1791	1	84	9	282	12	282	12	232	0	50	12	1992	2	1992	2	1925	0	67	2	43200	8	52
73	1	73	1	61	1	11	0	1875	10	1875	10	1804	0	71	10	274	12	274	12	224	2	49	10	1983	2	1983	2	1925	2	58	0	43200	9	52
77	1	77	1	70	1	6	0	1875	10	1875	10	1788	0	87	10	296	11	296	11	238	0	70	11	1988	2	1988	2	1905	1	63	1	43200	10	52
72	1	72	1	63	1	8	0	1875	10	1875	10	1808	1	67	9	415	12	338	12	319	1	24	11	1954	4	1954	4	1879	1	75	3	43200	1	53
80	1	80	1	74	0	5	1	1875	10	1875	10	1800	2	75	8	426	12	351	12	314	0	22	12	1924	2	1924	2	1862	0	61	2	43200	2	53
85	2	85	2	76	0	8	2	1875	10	1875	10	1786	1	89	9	410	12	349	12	314	2	20	10	1941	3	1941	3	1879	2	62	1	43200	3	53
75	2	75	2	70	0	4	2	1875	10	1875	10	1790	2	85	8	412	12	356	12	324	2	17	10	1953	2	1953	2	1887	2	66	0	43200	4	53
79	2	79	2	72	0	6	2	1875	10	1875	10	1806	0	69	10	407	12	355	12	314	1	26	11	1949	1	1949	1	1881	1	67	0	43200	5	53
86	2	86	2	77	0	9	2	1875	10	1875	10	1809	1	66	9	415	12	356	12	324	1	17	11	1945	2	1945	2	1884	1	60	1	43200	6	53
72	1	72	1	64	0	7	1	1875	10	1875	10	1790	1	85	9	414	12	352	12	312	0	25	12	1933	1	1933	1	1873	0	60	1	43200	7	53
78	2	78	2	69	1	8	1	1875	10	1875	10	1795	0	80	10	402	11	352	11	317	2	20	9	1948	3	1948	3	1890	3	58	0	43200	8	53
75	2	75	2	69	0	5	2	1875	10	1875	10	1801	4	74	6	448	11	349	11	313	1	21	10	1908	3	1908	3	1838	2	68	1	43200	9	53
73	2	73	2	62	0	10	2	1875	10	1875	10	1808	1	67	9	409	12	358	12	322	1	21	11	1948	2	1948	2	1888	1	60	1	43200	10	53
73	2	73	2	56	1	16	1	1875	10	1875	10	1799	0	76	10	257	11	257	11	213	0	44	11	2036	1	2036	1	1931	1	105	0	43200	1	54
73	1	73	1	64	0	9	1	1875	10	1875	10	1803	1	72	9	240	10	240	10	189	0	50	10	2019	2	2019	2	1925	2	94	0	43200	2	54
78	1	78	1	69	0	9	1	1875	10	1875	10	1821	1	54	9	222	10	222	10	177	0	45	10	2041	2	2041	2	1930	2	110	0	43200	3	54
78	2	78	2	72	1	5	1	1875	10	1875	10	1808	3	67	7	230	8	230	8	181	0	49	8	2037	4	2037	4	1926	4	111	0	43200	4	54
76	2	76	2	68	1	7	1	1875	10	1875	10	1806	1	69	9	254	10	254	10	206	0	48	10	2054	2	2054	2	1927	2	127	0	43200	5	54
75	2	75	2	66	0	8	2	1875	10	1875	10	1800	1	75	9	245	11	245	11	193	0	51	11	2032	1	2032	1	1923	1	109	0	43200	6	54
70	2	70	2	64	0	6	2	1875	10	1875	10	1800	0	75	10	234	12	234	12	191	0	42	12	2022	0	2022	0	1932	0	89	0	43200	7	54
77	2	77	2	67	1	9	1	1875	10	1875	10	1789	0	86	10	244	11	244	11	195	0	49	11	2015	1	2015	1	1926	1	89	0	43200	8	54
76	1	76	1	70	0	6	1	1875	10	1875	10	1796	2	79	8	256	9	256	9	211	0	45	9	2041	3	2041	3	1930	3	110	0	43200	9	54
73	2	73	2	63	0	9	2	1875	10	1875	10	1787	2	88	8	268	11	268	11	226	0	39	11	2045	2	2045	2	1933	1	112	1	43200	10	54
81	1	81	1	73	0	8	1	1875	10	1875	10	1803	2	72	8	342	9	342	9	315	4	22	5	2047	7	2047	7	1948	7	98	0	43200	1	55
79	2	79	2	71	0	7	2	1875	10	1875	10	1811	1	64	9	321	12	321	12	302	6	19	6	2056	6	2056	6	1956	6	100	0	43200	2	55

75	1	75	1	67	0	7	1	1875	10	1875	10	1794	0	81	10	330	11	330	11	311	5	19	6	2058	6	2058	6	1956	6	102	0	43200	3	55
80	2	80	2	69	0	10	2	1875	10	1875	10	1811	0	64	10	341	12	341	12	314	4	18	8	2056	4	2056	4	1947	4	108	0	43200	4	55
64	2	64	2	55	1	9	1	1875	10	1875	10	1799	2	76	8	338	9	338	9	321	4	17	5	2048	7	2048	7	1958	7	89	0	43200	5	55
72	1	72	1	63	0	9	1	1875	10	1875	10	1813	1	62	9	332	10	332	10	316	5	15	5	2089	7	2089	7	1959	7	109	0	43200	6	55
77	2	77	2	66	0	10	2	1875	10	1875	10	1790	0	85	10	341	12	341	12	319	5	22	7	2053	5	2053	5	1953	5	100	0	43200	7	55
77	1	77	1	70	0	6	1	1875	10	1875	10	1794	1	81	9	319	10	319	10	306	3	13	7	2057	5	2057	5	1962	5	95	0	43200	8	55
72	1	72	1	62	0	10	1	1875	10	1875	10	1791	2	84	8	334	10	334	10	320	4	13	6	2062	6	2062	6	1961	6	100	0	43200	9	55
77	2	77	2	70	0	6	2	1875	10	1875	10	1792	2	83	8	357	10	357	10	334	4	16	6	2079	6	2079	6	1952	6	127	0	43200	10	55
73	2	73	2	60	0	12	2	1875	10	1875	10	1791	2	84	8	293	11	293	11	212	1	80	10	1894	3	1894	3	1894	2	0	1	43200	1	56
80	2	80	2	69	1	10	1	1875	10	1875	10	1795	0	80	10	256	11	256	11	189	0	66	11	1909	1	1909	1	1908	1	1	0	43200	2	56
86	2	86	2	74	1	11	1	1875	10	1875	10	1805	3	70	7	230	10	230	10	197	0	52	10	1923	3	1923	3	1922	2	1	1	43200	3	56
72	1	72	1	59	0	12	1	1875	10	1875	10	1812	1	63	9	253	10	253	10	199	1	52	9	1922	3	1922	3	1921	3	1	0	43200	4	56
72	1	72	1	66	0	5	1	1875	10	1875	10	1815	0	60	10	232	11	232	11	180	0	52	11	1924	1	1924	1	1923	1	1	0	43200	5	56
80	2	80	2	73	0	6	2	1875	10	1875	10	1796	1	79	9	261	11	261	11	197	0	63	11	1912	1	1912	1	1911	1	1	0	43200	6	56
76	2	76	2	67	0	9	2	1875	10	1875	10	1808	0	67	10	247	12	247	12	190	0	57	12	1920	0	1920	0	1918	0	1	0	43200	7	56
74	1	74	1	65	0	9	1	1875	10	1875	10	1812	0	63	10	255	11	255	11	189	0	66	11	1911	1	1911	1	1909	1	1	0	43200	8	56
80	2	80	2	71	1	8	1	1875	10	1875	10	1798	0	77	10	243	11	243	11	183	0	60	11	1916	1	1916	1	1915	1	1	0	43200	9	56
75	0	75	0	68	0	7	0	1875	10	1875	10	1810	1	65	9	251	9	251	9	205	0	45	9	1931	3	1931	3	1929	3	1	0	43200	10	56
101	2	101	2	81	0	19	2	1875	10	1875	10	1796	0	79	10	167	12	167	12	147	0	19	12	1956	0	1956	0	1955	0	1	0	43200	1	57
101	2	101	2	85	0	15	2	1875	10	1875	10	1795	1	80	9	165	11	165	11	141	2	23	9	1952	3	1952	3	1951	3	1	0	43200	2	57
101	2	101	2	87	0	13	2	1875	10	1875	10	1799	0	76	10	148	12	148	12	127	0	20	12	1955	0	1955	0	1954	0	1	0	43200	3	57
101	2	101	2	85	0	15	2	1875	10	1875	10	1799	2	76	8	170	10	170	10	146	0	23	10	1952	2	1952	2	1951	2	1	0	43200	4	57
101	2	101	2	89	0	11	2	1875	10	1875	10	1802	3	73	7	149	9	149	9	132	0	15	9	1959	3	1959	3	1957	3	1	0	43200	5	57
101	2	101	2	90	1	10	1	1875	10	1875	10	1794	2	81	8	130	10	130	10	128	0	21	10	1953	3	1953	3	1953	2	0	1	43200	6	57
101	2	101	2	88	0	12	2	1875	10	1875	10	1803	0	72	10	151	12	151	12	136	0	15	12	1961	0	1961	0	1960	0	1	0	43200	7	57
101	2	101	2	86	0	14	2	1875	10	1875	10	1804	1	71	9	138	11	138	11	125	1	13	10	1963	2	1963	2	1962	2	1	0	43200	8	57
101	2	101	2	90	0	10	2	1875	10	1875	10	1804	1	71	9	142	11	142	11	122	0	19	11	1956	1	1956	1	1955	1	1	0	43200	9	57
101	2	101	2	92	0	8	2	1875	10	1875	10	1812	2	63	8	121	11	121	11	100	0	21	11	1954	2	1954	2	1954	1	0	1	43200	10	57
19	1	19	1	18	1	1	0	1875	10	1875	10	1786	1	89	9	372	9	351	9	314	1	22	8	1918	4	1918	4	1917	4	0	0	43200	1	58
28	0	28	0	28	0	0	0	1875	10	1875	10	1801	1	74	9	384	9	357	9	308	0	34	9	1900	3	1900	3	1899	3	0	0	43200	2	58
25	2	25	2	23	2	2	0	1875	10	1875	10	1787	0	88	10	396	11	349	11	310	0	24	11	1890	1	1890	1	1888	1	0	0	43200	3	58
29	0	29	0	26	0	2	0	1875	10	1875	10	1794	0	81	10	388	11	349	11	306	0	28	11	1893	1	1893	1	1893	1	0	0	43200	4	58
20	0	20	0	19	0	1	0	1875	10	1875	10	1781	2	94	8	405	8	356	8	311	2	30	6	1882	6	1882	6	1880	6	0	0	43200	5	58
33	0	33	0	33	0	0	0	1875	10	1875	10	1781	0	94	10	382	10	339	10	317	2	27	8	1911	4	1911	4	1910	4	0	0	43200	6	58
36	1	36	1	35	1	1	0	1875	10	1875	10	1784	2	91	8	358	9	349	9	313	0	21	9	1931	3	1931	3	1930	3	0	0	43200	7	58
27	0	27	0	25	0	2	0	1875	10	1875	10	1772	0	103	10	399	10	353	10	319	0	19	10	1896	2	1896	2	1895	2	0	0	43200	8	58
24	0	24	0	21	0	2	0	1875	10	1875	10	1777	2	98	8	386	10	358	10	310	1	33	9	1899	3	1899	3	1899	3	0	0	43200	9	58
24	1	24	1	22	1	2	0	1875	10	1875	10	1795	1	80	9	368	10	366	10	320	0	31	10	1928	2	1928	2	1928	2	0	0	43200	10	58
26	1	26	1	23	0	2	1	1875	10	1875	10	1782	0	93	10	239	11	239	11	182	0	57	11	1918	1	1918	1	1918	1	0	0	43200	1	59
30	0	30	0	28	0	2	0	1875	10	1875	10	1777	0	98	10	248	10	248	10	169	0	79	10	1897	2	1897	2	1896	2	0	0	43200	2	59
19	0	19	0	19	0	0	0	1875	10	1875	10	1754	0	121	10	262	10	262	10	194	0	68	10	1908	2	1908	2	1907	2	0	0	43200	3	59
28	1	28	1	24	0	4	1	1875	10	1875	10	1790	0	85	10	237	11	237	11	168	0	69	11	1907	1	1907	1	1906	1	0	0	43200	4	59
38	1	38	1	33	0	4	1	1875	10	1875	10	1779	0	96	10	229	11	229	11	175	3	54	8	1921	4	1921	4	1921	4	0	0	43200	5	59

25	0	25	0	24	0	1	0	1875	10	1875	10	1775	1	100	9	241	9	241	9	163	1	78	8	1898	4	1898	4	1897	4	0	0	43200	6	59
22	1	22	1	21	1	1	0	1875	10	1875	10	1783	1	92	9	227	10	227	10	170	0	57	10	1919	2	1919	2	1918	2	0	0	43200	7	59
21	0	21	0	18	0	2	0	1875	10	1875	10	1799	0	76	10	209	10	209	10	138	2	51	8	1924	4	1924	4	1924	4	0	0	43200	8	59
26	1	26	1	22	0	4	1	1875	10	1875	10	1780	0	95	10	219	11	219	11	174	0	45	11	1931	1	1931	1	1930	1	0	0	43200	9	59
16	0	16	0	15	0	1	0	1875	10	1875	10	1770	1	105	9	231	10	231	10	164	0	67	10	1909	2	1909	2	1908	2	0	0	43200	10	59
26	0	26	0	24	0	2	0	1875	10	1875	10	1793	0	82	10	309	10	309	10	306	7	3	3	2069	9	2069	9	1972	9	96	0	43200	1	60
31	0	31	0	29	0	1	0	1875	10	1875	10	1789	1	86	9	311	10	311	10	306	7	5	3	2066	9	2066	9	1970	9	96	0	43200	2	60
29	0	29	0	25	0	4	0	1875	10	1875	10	1783	1	92	9	334	11	334	11	330	7	4	4	2073	9	2073	9	1971	8	101	1	43200	3	60
19	1	19	1	18	1	1	0	1875	10	1875	10	1774	0	101	10	363	10	351	10	331	6	5	4	2069	8	2069	8	1943	8	125	0	43200	4	60
32	1	32	1	28	1	3	0	1875	10	1875	10	1799	1	76	9	309	11	309	11	302	7	6	4	2086	8	2086	8	1968	8	118	0	43200	5	60
19	1	19	1	17	1	2	0	1875	10	1875	10	1791	0	84	10	311	12	311	12	310	8	1	4	2078	9	2078	9	1974	8	103	1	43200	6	60
31	0	31	0	27	0	4	0	1875	10	1875	10	1776	1	99	9	327	9	327	9	321	6	6	3	2065	9	2065	9	1969	9	95	0	43200	7	60
32	1	32	1	31	1	1	0	1875	10	1875	10	1792	0	83	10	317	10	317	10	317	6	0	4	2067	8	2067	8	1975	8	91	0	43200	8	60
22	1	22	1	21	1	1	0	1875	10	1875	10	1772	0	103	10	324	11	324	11	323	8	1	3	2066	9	2066	9	1973	9	91	0	43200	9	60
24	1	24	1	23	1	0	0	1875	10	1875	10	1786	0	89	10	333	10	333	10	326	6	4	4	2062	8	2062	8	1968	8	114	0	43200	10	60
28	1	28	1	27	0	1	1	1875	10	1875	10	1800	1	75	9	466	10	345	10	247	1	83	9	1847	3	1847	3	1755	3	90	0	43200	1	61
26	2	26	2	23	0	3	2	1875	10	1875	10	1785	0	90	10	479	12	353	12	249	1	89	11	1842	1	1842	1	1743	1	96	0	43200	2	61
30	0	30	0	29	0	1	0	1875	10	1875	10	1773	2	102	8	462	11	355	11	252	0	88	11	1862	1	1862	1	1765	1	96	0	43200	3	61
22	0	22	0	19	0	3	0	1875	10	1875	10	1791	0	84	10	439	10	355	10	266	1	74	9	1871	3	1871	3	1782	3	88	0	43200	4	61
23	0	23	0	19	0	3	0	1875	10	1875	10	1793	0	82	10	475	10	366	10	268	0	83	10	1864	2	1864	2	1768	2	96	0	43200	5	61
25	1	25	1	22	0	3	1	1875	10	1875	10	1789	2	86	8	448	11	349	11	249	0	85	11	1872	1	1872	1	1776	1	95	0	43200	6	61
29	0	29	0	25	0	4	0	1875	10	1875	10	1793	2	82	8	469	10	363	10	270	0	78	10	1886	2	1886	2	1776	2	109	0	43200	7	61
19	0	19	0	18	0	1	0	1875	10	1875	10	1778	0	97	10	489	10	350	10	261	0	74	10	1830	2	1830	2	1747	2	82	0	43200	8	61
16	0	16	0	14	0	1	0	1875	10	1875	10	1779	1	96	9	496	9	368	9	280	0	73	9	1856	3	1856	3	1759	3	97	0	43200	9	61
22	0	22	0	19	0	3	0	1875	10	1875	10	1798	1	77	9	447	10	348	10	258	0	75	10	1876	2	1876	2	1786	2	89	0	43200	10	61
22	0	22	0	20	0	1	0	1875	10	1875	10	1791	0	84	10	319	12	319	12	312	3	6	9	2044	5	2044	5	1968	3	76	2	43200	1	62
21	0	21	0	18	0	2	0	1875	10	1875	10	1785	2	90	8	334	12	334	12	328	2	5	10	2046	5	2046	5	1969	2	77	3	43200	2	62
25	1	25	1	19	0	6	1	1875	10	1875	10	1782	0	93	10	296	12	296	12	291	2	5	10	2032	3	2032	3	1970	2	61	1	43200	3	62
34	0	34	0	32	0	2	0	1875	10	1875	10	1783	0	92	10	284	12	284	12	279	0	5	12	2026	1	2026	1	1970	0	55	1	43200	4	62
26	1	26	1	25	0	1	1	1875	10	1875	10	1786	1	89	9	317	11	317	11	310	0	7	11	2041	2	2041	2	1968	1	72	1	43200	5	62
20	0	20	0	19	0	1	0	1875	10	1875	10	1773	2	102	8	307	12	307	12	302	3	5	9	2022	6	2022	6	1970	3	51	3	43200	6	62
13	1	13	1	11	0	1	1	1875	10	1875	10	1790	1	85	9	304	12	304	12	297	1	7	11	2048	1	2048	1	1968	1	80	0	43200	7	62
23	1	23	1	19	0	3	1	1875	10	1875	10	1773	1	102	9	338	12	338	12	329	1	7	11	2026	3	2026	3	1965	1	60	2	43200	8	62
28	0	28	0	22	0	5	0	1875	10	1875	10	1779	2	96	8	338	12	338	12	329	2	7	10	2042	6	2042	6	1966	2	76	4	43200	9	62
29	0	29	0	25	0	4	0	1875	10	1875	10	1782	0	93	10	321	12	321	12	313	2	8	10	2041	4	2041	4	1967	2	73	2	43200	10	62
26	1	26	1	22	0	4	1	1875	10	1875	10	1782	1	113	9	456	12	352	12	253	0	84	12	1827	1	1827	1	1771	0	54	1	43200	1	63
20	2	20	2	18	0	2	2	1875	10	1875	10	1774	0	101	10	418	12	355	12	271	0	69	12	1893	0	1893	0	1828	0	64	0	43200	2	63
27	0	27	0	25	0	2	0	1875	10	1875	10	1795	1	80	9	404	12	359	12	280	0	84	12	1901	3	1901	3	1831	0	69	3	43200	3	63
17	0	17	0	17	0	0	0	1875	10	1875	10	1790	1	85	9	446	11	359	11	258	1	86	10	1876	4	1876	4	1786	2	88	2	43200	4	63
25	0	25	0	23	0	2	0	1875	10	1875	10	1796	1	79	9	418	11	361	11	280	0	86	11	1882	3	1882	3	1818	1	64	2	43200	5	63
19	0	19	0	18	0	1	0	1875	10	1875	10	1792	1	83	9	424	11	348	11	259	1	74	10	1878	4	1878	4	1809	2	67	2	43200	6	63
30	0	30	0	29	0	1	0	1875	10	1875	10	1767	0	108	10	477	12	366	12	262	0	89	12	1840	2	1840	2	1758	0	79	2	43200	7	63
34	2	34	2	29	0	5	2	1875	10	1875	10	1789	0	86	10	434	12	346	12	254	0	77	12	1872	0	1872	0	1796	0	76	0	43200	8	63

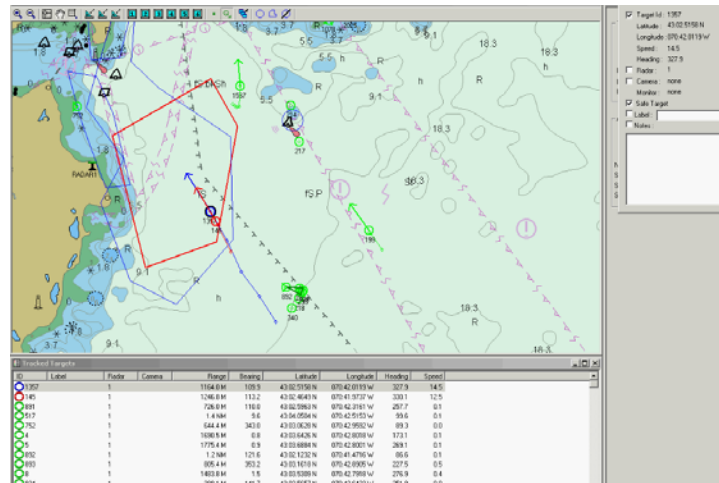
27	1	27	1	23	0	4	1	1875	10	1875	10	1780	1	95	9	435	12	357	12	253	0	89	12	1883	2	1883	2	1793	0	69	2	43200	9	63
22	0	22	0	19	0	3	0	1875	10	1875	10	1784	0	91	10	449	12	356	12	259	2	82	10	1845	4	1845	4	1786	2	59	2	43200	10	63
27	0	27	0	26	0	1	0	1875	10	1875	10	1775	1	100	9	545	12	352	12	322	9	15	3	1890	11	1890	11	1752	9	137	2	43200	1	64
12	1	12	1	8	0	3	1	1875	10	1875	10	1790	2	85	8	529	12	343	12	310	8	18	4	1922	11	1922	11	1756	8	166	3	43200	2	64
26	0	26	0	25	0	1	0	1875	10	1875	10	1782	0	93	10	499	12	330	12	321	11	14	1	1930	13	1930	13	1797	11	152	2	43200	3	64
27	2	27	2	21	0	5	2	1875	10	1875	10	1787	0	88	10	537	12	363	12	332	10	16	2	1943	10	1943	10	1770	10	173	0	43200	4	64
17	1	17	1	16	0	1	1	1875	10	1875	10	1787	0	88	10	543	12	354	12	326	9	13	3	1916	10	1916	10	1758	9	157	1	43200	5	64
29	0	29	0	24	0	4	0	1875	10	1875	10	1762	0	113	10	556	12	357	12	325	10	17	2	1907	12	1907	12	1744	10	163	2	43200	6	64
22	0	22	0	20	0	1	0	1875	10	1875	10	1773	1	102	9	549	11	359	11	331	6	13	5	1918	7	1918	7	1757	7	161	0	43200	7	64
19	2	19	2	17	0	2	2	1875	10	1875	10	1786	1	89	9	529	12	353	12	323	11	15	1	1931	12	1931	12	1768	11	161	1	43200	8	64
21	1	21	1	18	0	2	1	1875	10	1875	10	1783	0	92	10	496	12	355	12	325	10	15	2	1947	11	1947	11	1803	10	143	1	43200	9	64
25	0	25	0	22	0	3	0	1875	10	1875	10	1786	0	89	10	527	12	354	12	324	8	15	4	1923	10	1923	10	1772	8	150	2	43200	10	64
19	0	19	0	18	0	1	0	1875	10	1875	10	1779	2	96	8	381	10	380	10	245	0	100	10	1985	4	1985	4	1839	2	145	2	43200	1	65
16	1	16	1	14	0	2	1	1875	10	1875	10	1794	0	81	10	392	12	350	12	230	1	105	11	1981	2	1981	2	1812	1	167	1	43200	2	65
27	1	27	1	24	0	3	1	1875	10	1875	10	1797	1	78	9	394	12	342	12	227	0	100	12	1980	2	1980	2	1807	0	171	2	43200	3	65
23	1	23	1	17	0	6	1	1875	10	1875	10	1781	0	94	10	397	11	356	11	226	1	115	10	1979	2	1979	2	1804	2	174	0	43200	4	65
25	0	25	0	24	0	0	0	1875	10	1875	10	1789	0	86	10	370	11	357	11	230	1	92	10	2016	3	2016	3	1855	2	161	1	43200	5	65
20	1	20	1	18	0	2	1	1875	10	1875	10	1770	0	105	10	387	12	359	12	235	0	109	12	1979	1	1979	1	1823	0	155	1	43200	6	65
29	0	29	0	27	0	2	0	1875	10	1875	10	1792	0	83	10	371	12	350	12	243	0	92	12	2021	2	2021	2	1847	0	173	2	43200	7	65
33	0	33	0	27	0	6	0	1875	10	1875	10	1791	0	84	10	387	12	352	12	245	0	92	12	1995	2	1995	2	1833	0	161	2	43200	8	65
24	0	24	0	18	0	5	0	1875	10	1875	10	1789	0	86	10	378	12	358	12	233	0	110	12	1991	2	1991	2	1830	0	161	2	43200	9	65
20	1	20	1	19	0	1	1	1875	10	1875	10	1779	0	96	10	382	12	371	12	257	0	99	12	2021	1	2021	1	1830	0	170	1	43200	10	65

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX J: HARBORGUARD TEST PLAN

OA – 4603 TEST PLANNING PROJECT

TEST PLAN FOR HarborGuard



LCDR Joseph Torian
LCDR Dale Johnson
LT Morgan Ames
Henry Nguyen
Horn Lim

TABLE OF CONTENTS

Section	Description	Page
1	Introduction to the Project	3
2	Mission Need and Operational Requirements	3
2.1	Mission Need	3
2.2	Operational Requirements	4
3	Scope of the Evaluation	5
3.1	Critical Technical Parameters	6
3.2	General Function and Capability Dendritics	7
3.3	Critical Operational Issues	8
3.4	Measures of Effectiveness/ Suitability and Measures of Performance	8
3.5	Test Objective Matrix	13
3.6	General Test Operations, Test Vehicles and Scenario Overview	14
4	Operational Effectiveness	15
4.1	Scenarios	15
4.2	E-Test	18
5	Operational Suitability	22
5.1	S-Test	22

Annexes	Description	Page
A	Resource Requirements	24
B	Data Sheets and Questionnaires	25
C	Omitted	-
D	Data Analysis Plan	31

SECTION 1 – Introduction to the Project

1.1 Purpose

The purpose of this project is to plan the testing requirements for the HarborGuard System. The aim of the project is to develop a combined Development Test (DT) and Operational Test (OT) Test plan. In addition, a methodology will be generated that will provide a sequence of steps to follow in order to obtain, verify and provide data for assessment on the performance, suitability and relevancy of the HarborGuard System.

1.2. System Description

The HarborGuard integrated waterside security and surveillance system provides high performance sonar, radar sensors, Automatic Identification System (AIS) and Closed Circuit Television (CCTV) for tracking vessels, swimmers and suspicious underwater objects. This system can be adapted as a waterside security solution for both military and commercial customers worldwide. The US Navy can provide effective port security for a wide variety of scenarios including those for domestic and foreign installations. It provides real-time situational awareness for Ports, Harbors and offshore facilities. HarborGuard uses the latest technology to provide the most capable measures and cost effective solutions for Waterside Security applications.

SECTION 2 – Mission Need and Operational Requirements

2.1 Mission Need

Port Security is a very high interest area of concern for the United States and many of the World's leading economies that depend on ports for trade and commerce. Ports are critical gateways for the movement of international commerce. More than 95 percent of our non-North American foreign trade (and 100 percent of certain commodities, such as foreign oil, on which we are heavily dependent) arrives by ship. This tremendous flow of goods creates many kinds of vulnerabilities. Drugs and illegal aliens are routinely smuggled into this country, not only in small boats but also hidden among otherwise legitimate cargoes on large commercial ships. These same pathways are available for exploitation by a terrorist organization or any nation or person wishing to attack us surreptitiously. Protecting against these vulnerabilities is made more difficult by the tremendous number and variety of U.S. ports. Some are multibillion-dollar enterprises, while others have very limited facilities and very little traffic.

Therefore there is a critical need for a system such as HarborGuard to alleviate or remove these threats.

2.2 Operational Requirements

The following is a list of operational requirements for the HarborGuard System:

- a. HarborGuard shall integrate all sensors into a Common Operating Picture for an accurate portrayal of real time events to develop domain awareness.
- b. HarborGuard shall provide remote control operations of all sensors.
- c. HarborGuard shall provide selectable Security Zone layers based on threat conditions.
- d. HarborGuard shall generate alarms based on threat criteria.
- e. HarborGuard shall provide continuous logging of target tracks and alarm data for playback and analysis.
- f. HarborGuard shall enable automatic camera tracking of targets.
- g. HarborGuard shall stop small surface threat of size up to 5 tons.
- h. HarborGuard shall be able to transmit verbal warnings to deter inadvertent intruders.
- i. HarborGuard shall detect and track swimmer size surface targets.
- j. HarborGuard shall be able to identify detected targets.
- k. HarborGuard shall provide monitoring of all transponder-equipped vessels.
- l. HarborGuard shall provide detection and tracking of underwater targets including Autonomous Underwater Vehicles (AUVs).
- m. HarborGuard shall be able to detect the presence of suspicious objects on the sea floor.

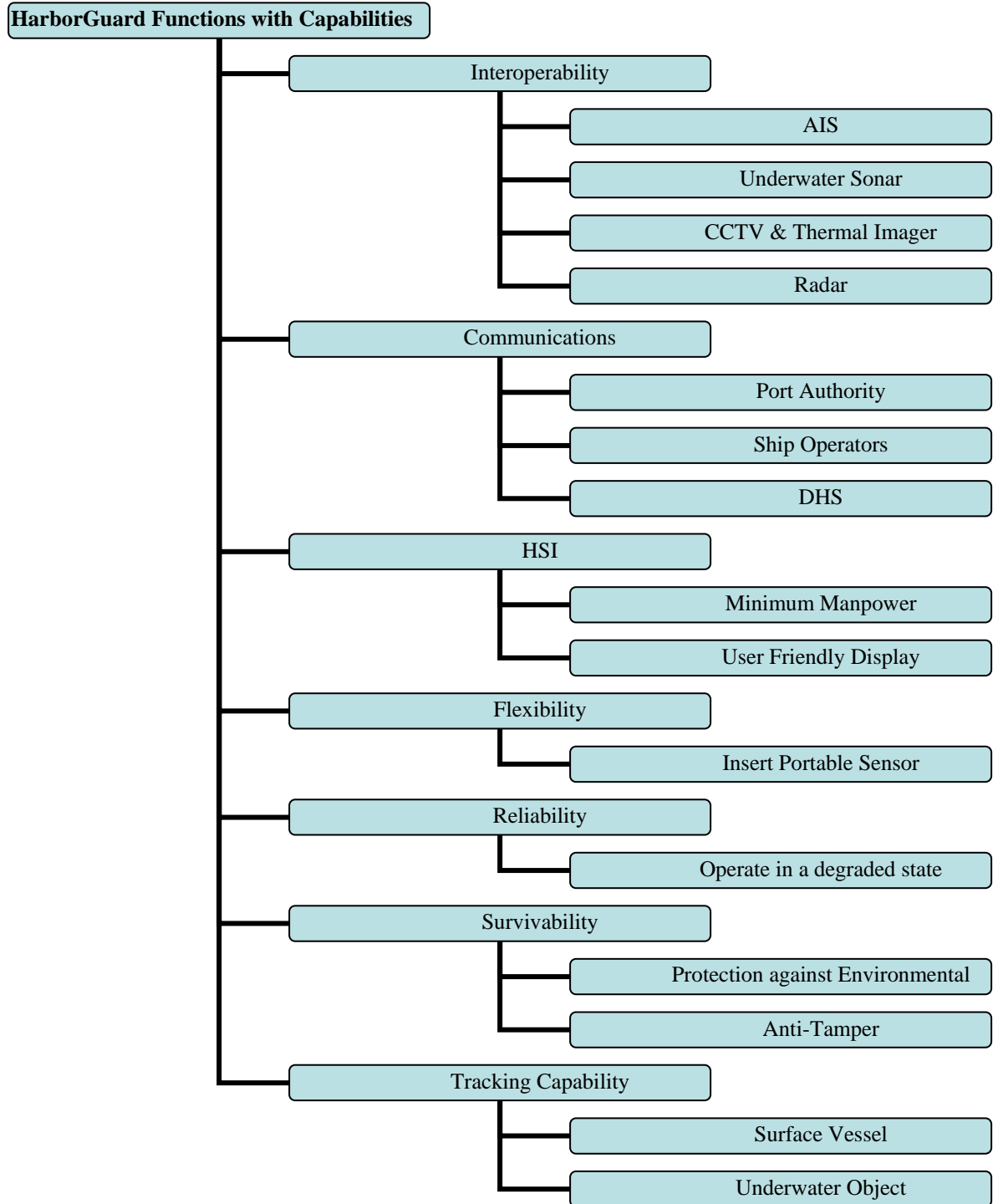
SECTION 3 – Scope of the Evaluation

3.1 Critical Technical Parameters

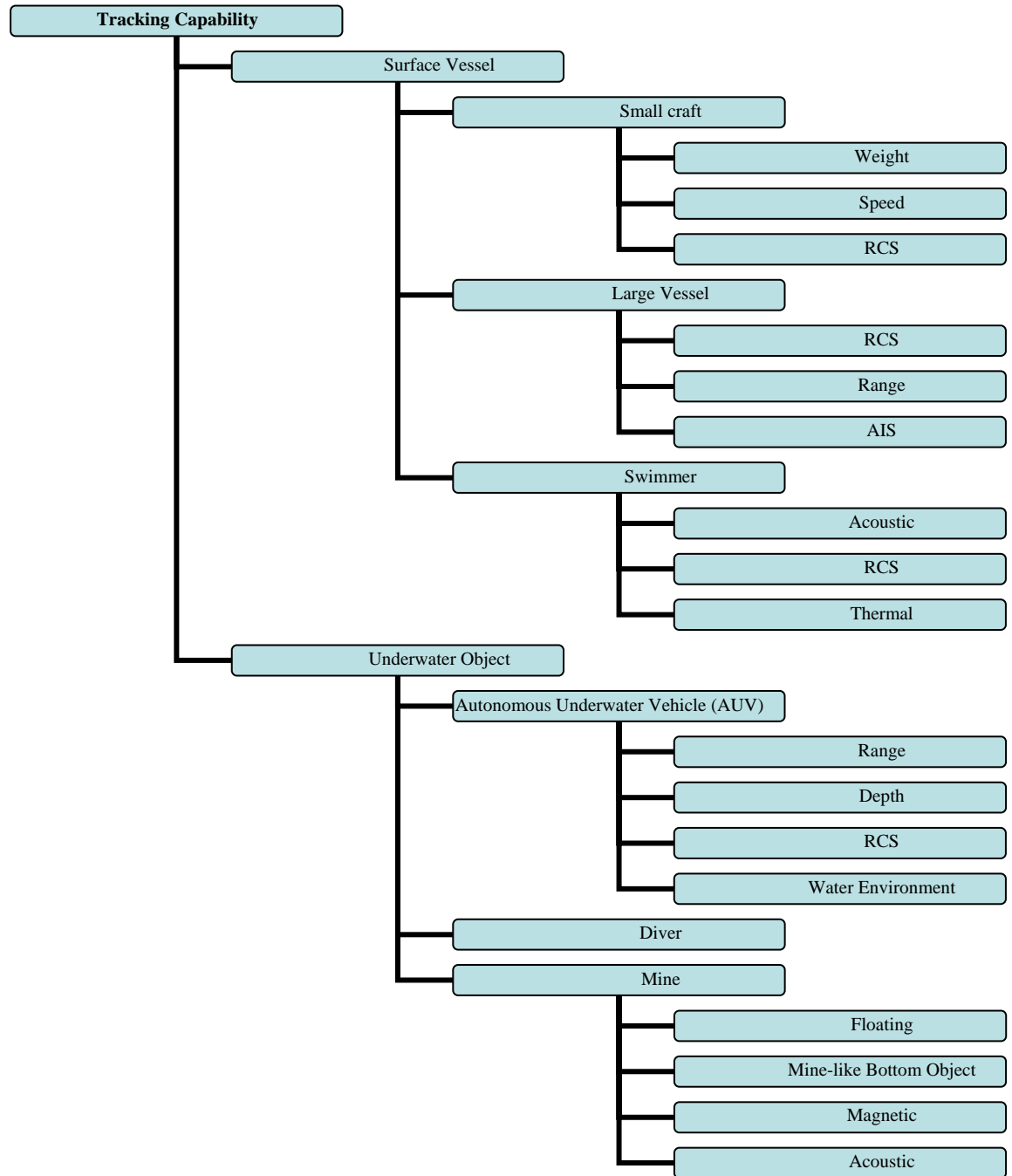
Capability	Technical Parameter	Performance Criteria
Tracking Capability	Tracking Capacity	>= 1000 tracks
	Range Resolution	3.5 m
	Azimuth Resolution	2 mrad
Detection Capability	Search rate	80 rpm
	Average Detection Range (small boat)	14.6 km
	Probability of Detection (small target)	0.85
Data Processing Capability	Average Transmit Time	< 100 ms
	Average Retrieval Time	< 150 ms
	Average speed network file transfer	> 1 Gbps
Monitoring Transponder Vessels	Signal Reception Range	> 27.4 km
Detection of Objects on Sea Floor	Detection Depth	> 20 m
	Detection Range	> 2 km
	RCS	> 0.1 m ²
Warning Capability	Signal Strength	> 85dBA @ 1 km
Sea Fence Capability	Kinetic Dissipation	> 2160 KJ
Identification Capability	Minimum # of resolvable lines across minimum dimension	> 12.8 resels
Response Capability	Average Time required to Respond to Threat	< 3 min
Acoustic Sensitivity	Underwater Transmission Level	> 40 dB
Interoperability	Number of messages transmitted	>150 messages per second

General Function and Capability Dendritics

3.1.1 General Function Dendritic



3.1.2 Capability Dendritic (Tracking Capability)



3.3 Critical Operational Issues

- 3.3.1 COI 1 – Is the HarborGuard System able to track all targets detected by the sensors in the operational area?
- 3.3.2 COI 2 – Can the HarborGuard System detect and track swimmer size surface targets?
- 3.3.3 COI 3 – Is the HarborGuard System able to record and playback target tracks and alarm data for analysis?
- 3.3.4 COI 4 – Can the HarborGuard System provide monitoring of all transponder equipped vessels?
- 3.3.5 COI 5 – Can the HarborGuard System detect suspicious objects on the sea floor?
- 3.3.6 COI 6 – Can the HarborGuard System transmit verbal warnings to intruders?
- 3.3.7 COI 7 – Can the HarborGuard System stop small surface threats?
- 3.3.8 COI 8 – Can the HarborGuard System identify detected targets?
- 3.3.9 COI 9 – Is the HarborGuard System able to respond appropriately when threat levels are changed?
- 3.3.10 COI 10 – Can the HarborGuard System detect and track Autonomous Underwater Vehicle(AUV)?
- 3.3.11 COI 11 – (Human Factors) Can the HarborGuard System be manned by 2 operators?
- 3.3.12 COI 12 – (Interoperability) Is the HarborGuard System able to integrate all existing sensors into an easily interpreted domain awareness?

3.4 Measures of Effectiveness/ Suitability and Measures of Performance

- 3.4.1 COI 1 – Is the HarborGuard System able to track all targets detected by the sensor in the operational area?
 - MOE 3.4.1.1 Probability of targets track
 - MOP 3.4.1.1.1 Percentage of targets track
 - DR3.4.1.1.1.1 Coverage area
 - DR3.4.1.1.1.2 Max number of targets track
 - DR3.4.1.1.1.3 Number of targets track
 - DR3.4.1.1.1.4 Target size
 - MOE 3.4.1.2 Probability of targets track lost
 - MOP 3.4.1.2.1 Percentage of track lost
 - DR3.4.1.2.1.1 Time of track lost
 - DR3.4.1.2.1.2 Target ID of Track lost
 - MOP 3.4.1.2.2 Target resolution
 - MOP 3.4.1.2.3 Size of target

3.4.2 COI 2 – Can the HarborGuard System detect and track swimmer size target?

MOE 3.4.2.1 Proportion of targets detected

MOP 3.4.2.1.1 Number of targets detected

DR3.4.2.1.1.1 Range of detection

DR3.4.2.1.1.2 Time from target entry into monitored area until detection

DR3.4.2.1.1.3 Average target acquisition time

MOE 3.4.2.2 False detection

MOP 3.4.2.2.1 False alarm rate (Type II error)

3.4.3 COI 3 – Is the HarborGuard System able to record and playback target tracks and alarm data for analysis?

MOE 3.4.3.1 Recording Capability

MOP 3.4.3.1.1 Recording capacity

DR3.4.3.1.1.1 Number of tracks recorded

DR3.4.3.1.1.2 Maximum time of recording

DR3.4.3.1.1.3 Speed of recording

MOP 3.4.3.1.2 Recording quality

MOE 3.4.3.2 Storage capacity

MOP 3.4.3.2.1 Number of tracks stored

MOP 3.4.3.2.2 Capacity of time store

MOE 3.4.3.3 Playback Capability

3.4.4 COI 4 – Can the HarborGuard system provide monitoring of all transponder equipped vessels?

MOE 3.4.4.1 Monitoring Capability

MOP 3.4.4.1.1 Mean Variance of monitoring range

DR3.4.4.1.1.1 Position of ship

DR3.4.4.1.1.2 Range of ship

MOP 3.4.4.1.2 Percentage of dropped transponder equipped vessels from the system

DR3.4.4.1.2.1 Number of tracks lost

DR3.4.4.1.2.2 Average time to reacquire a dropped transponder equipped vessel

3.4.5 COI 5 – Can the HarborGuard system detect suspicious objects on the sea floor?

MOE 3.4.5.1 Detection Capability

MOP 3.4.5.1.1 Mean Variance of detection range

DR3.4.5.1.1.1 Number of targets

DR3.4.5.1.1.2 Orientation of object to sensor

MOE 3.4.5.2 Probability of detecting a false object

MOP 3.4.5.2.1 Percentage of False contacts

DR3.4.5.2.1.1 Distance

DR3.4.5.2.1.2 Resolution

DR3.4.5.2.1.3 Time

3.4.6 COI 6 –Can the HarborGuard system communicate verbal warnings to intruders?

MOE 3.4.6.1 Capability to broadcast

MOP 3.4.6.1.1 Signal Quality

DR3.4.6.1.1.1 Broadcast Signal to Noise Ratio (S/N).

DR3.4.6.1.1.2 Decibel level at 100, 200, 500, 1000, 1500 and 2000m

DR3.4.6.1.1.3 Cone of useable signal strength

DR3.4.6.1.1.4 Broadcast power level

MOE 3.4.6.2 Ability to broadcast in languages specific to the region

MOP 3.4.6.2.1 Percentage of foreign boat operators that are able to understand the broadcast message.

3.4.7 COI 7 – Can the HarborGuard system stop small surface threats?

MOE 3.4.7.1 Ability to fully restrain a 5 ton small boat moving at 60 knots.

MOP 3.4.7.1.1 Percentage of attacks by a 5 ton boat that penetrate the barrier and are not stopped

DR3.4.7.1.1.1 Boat weight

DR3.4.7.1.1.2 Boat speed

DR3.4.7.1.1.3 Angle of attack

DR3.4.7.1.1.4 Time to fully restrain boat

DR3.4.7.1.1.5 Average Distance traveled by the boat before stopping

3.4.8 COI 8 – Can the HarborGuard System identify detected targets?

MOE 3.4.8.1 Identification Capability

MOP 3.4.8.1.1 Average Time from Detection to Identification

DR3.4.8.1.1.1 Time at detection

DR3.4.8.1.1.2 Time at Identification

MOP 3.4.8.1.2 Average Range of Identification

MOE 3.4.8.2 Probability of Identification

MOP 3.4.8.2.1 Proportion of Correct Identification

3.4.9 COI 9 – Is the HarborGuard System able to respond based on different threat levels?

MOE 3.4.9.1 Responsive Capability

MOP 3.4.9.1.1 Average Time taken to respond to threat

DR3.4.9.1.1.1 Time at threat identification

DR3.4.9.1.1.2 Time at response initiation

DR3.4.9.1.1.3 Time at threat neutralization

MOP 3.4.9.1.2 Available Time to respond to threat

- 3.4.10 COI 10 – Can the HarborGuard system detect and track AUVs?
 - MOE 3.4.10.1 Probability of detecting AUV
 - MOP 3.4.10.1.1 Ratio of AUVs detected to AUVs missed
 - DR3.4.10.1.1.1 Number of AUVs detected
 - DR3.4.10.1.1.2 Number of AUVs totally missed
 - DR3.4.10.1.1.3 Range of AUVs when detected
 - MOE 3.4.10.2 Probability of tracking detected AUVs
 - MOP 3.4.10.2.1 Ratio of AUVs tracked to those track lost
 - DR3.4.10.2.1.1 Number of AUVs tracked
 - DR3.4.10.2.1.2 Number of AUV tracks that were lost
 - DR3.4.10.2.1.3 Time from detection until track is lost
- 3.4.11 COI 11 – (Human Factors) Can the HarborGuard system be sufficiently manned by two operators?
 - MOE 3.4.11.1 Probability of operators missing a contact of interest shown on one of the displays
 - MOP 3.4.11.1.1 Percentage of contacts on the displays the operators cannot adequately describe during a task saturated environment
 - DR3.4.11.1.1.1 Number of contacts on the display
 - DR3.4.11.1.1.2 Number of contacts the operators have sufficient knowledge
 - DR3.4.11.1.1.3 The time required for operators to react to threats
 - MOE 3.4.11.2 Capability of the operators to maintain a consistent level of performance regardless of state of fatigue
 - MOP 3.4.11.2.1 Percentage of successful target interrogations at the beginning of the watch compared to those at the end of the watch
 - DR3.4.11.2.1.1 Number of successful interrogations at the beginning of watch
 - DR3.4.11.2.1.2 Number of total interrogations at the beginning of watch
 - DR3.4.11.2.1.3 Number of successful interrogations at the end of watch
 - DR3.4.11.2.1.4 Number of total interrogations at the end of watch
- 3.4.12 COI 12 – (Interoperability) Is the HarborGuard system able to integrate all existing sensors into an easily understood and interpreted domain awareness?
 - MOE 3.4.12.1 The capability of systems to be successfully integrated
 - MOP 3.4.12.1.1 Percentage of sensors integrated at one time

- DR3.4.12.1.1.1 Number of sensors integrated at one time
- DR3.4.12.1.1.2 Number of sensors missed due to system limitations
- DR3.4.12.1.1.3 The number of sensors transmitting data at certain moments
- MOE 3.4.12.2 The transmission capability of the sensors for integration
 - MOP 3.4.12.2.1 Average Transmission backlog
 - DR3.4.12.2.1.1 Transmission rate of the sensors
 - DR3.4.12.2.1.2 Receiving rate of the receptors
 - DR3.4.12.2.1.3 Time from initial detection until correct display

3.5 Test Objective Matrix

COI	Test Objectives and Sub-Objectives	Test
1.Tracking Capability	To determine the tracking capability of the HarborGuard <ul style="list-style-type: none"> • Number of targets tracked E-1a • Size of targets tracked E-1b • Coverage area E-1c 	E-1
2.Detection Capability	To determine the detection capability of the HarborGuard <ul style="list-style-type: none"> • Range of detection E-2a • Average time from target presentation to detection E-2b 	E-2
3.Data Processing Capability	To determine the data processing capability of the HarborGuard <ul style="list-style-type: none"> • Number of tracks recorded E-3a • Number of tracks stored E-3b 	E-3
4.Monitor transponder vessels	To determine compatibility of transponder equipment with HarborGuard. <ul style="list-style-type: none"> • Monitoring Capability E-4a 	E-4
5.Detection objects on sea floor	To determine detection range and probability of false object. <ul style="list-style-type: none"> • Mean variance detection E-5a • Percentage of false contacts E-5b 	E-5
6.Warning Capability	To assess the effectiveness of verbal warnings. <ul style="list-style-type: none"> • Signal to Noise Ratio E-6a 	E-6
7.Sea Fence Capability	To assess the ability to stop surface threats. <ul style="list-style-type: none"> • Number of successful stops to a 5-ton boat attack E-7a 	E-7

8. Identification Capability	To determine the identification capability of the CCTV and Thermal Imager <ul style="list-style-type: none"> • Range of identification E-8a • Ratio of correct identification E-8b • Time taken to perform identification E-8c 	E-8
9. Responsive Capability	To determine the ability to respond to different threat levels <ul style="list-style-type: none"> • Time available to respond E-9a • Average response time E-9b 	E-9
10. Acoustic Sensitivity	To assess the ability to detect AUV <ul style="list-style-type: none"> • Detection Range E-10a • Noise generated by the AUV E-10b 	E-10
11. (Human Factors) Crew Size	To determine the effectiveness of the crew size in performing the required tasks <ul style="list-style-type: none"> • Crew of 2 S-1a • Crew of 3 S-1b 	S-1
12. Interoperability	To determine the interoperability with other hardware. <ul style="list-style-type: none"> • Wireless communications S-2a • Wire transmissions S-2b • Digital/Analog S-2c 	S-2

3.6 General Test Operations, Test Vehicles and Scenario Overview

3.6.1 Scenario Overview

- Scenario A: Defending against AUV
- Scenario B: Small Boat Attack on Critical Infrastructure
- Scenario C: Detect and track large vessel
- Scenario D: Detect and track surface and subsurface swimmers.

3.6.2 Instrumentation Requirements

The list below shows a list of the additional equipments needed for each scenario.

	Additional Equipments
Scenario A	AUVs, Launching platform, dummy bottom mine, GPS, Mk 107 Mod 0 Hydrographic mapping Unit
Scenario B	3 5-ton boats, Notice to Mariners, LRAD, Sea Barrier, GPS
Scenario C	AIS equipped Large Vessel, GPS
Scenario D	Scuba Diver, Surface Swimmer, GPS

3.6.3 Limitation to Scope of Test

- a. Realism – The use of actual mines for HarborGuard to detect on the sea floor. [Limited Effectiveness Evaluation]
- b. Uncontrollable Boat Traffic – The presence of commercial and pleasure craft in the testing area. [Limited Tactical Evaluation]
- c. Test Operator Proficiency – Uniqueness of the system limits the operators' evaluation. [Limits HSI Evaluation]
- d. Threat Neutralization – Limited use of LRAD to avoid harm to test participants. [Limited Tactical Evaluation]

SECTION 4 – Operational Effectiveness

4.1 Scenarios and Run Profiles

4.1.1 Scenario A : Defending against AUV threat

4.1.1.1 Overview

- a. Scenario begins with two AUVs launched from an anchored ship in the Oakland harbor that is awaiting port entrance.
- b. The AUVs mission is to penetrate HarborGuard undetected, to plant an explosive on a large container ship berthed at the pier and to deploy a bottom mine in the shipping channel near the port.
- c. The HarborGuard mission is to detect and track the AUVs. The system will alert the operator and notify the appropriate agencies of the perceived threat.



Figure 1: Scenario A- Defending against AUV threat

4.1.1.2 Run Profile

- a. The launching ship will be anchored at one nautical mile from the Port of Oakland.
- b. A large container ship will be berthed at pier 37 at 0000.
- c. AUV 1 carrying explosives will be launched at 0100.
- d. AUV 1 will cruise at 3 knots towards the large container ship in a direct path and attempt to attach the explosives to the container ship.
- e. AUV 2 carrying a bottom mine will be launched at 0130.
- f. AUV 2 will move to the shipping channel near the port and attempt to deploy the bottom mine.
- g. HarborGuard will attempt to detect the two AUVs and to maintain the tracks.
- h. HarborGuard will attempt to identify the AUVs as perceived threats and notify the appropriate agencies.
- i. HarborGuard will attempt to detect the suspicious object planted by AUV 2.
- j. The launching ship will attempt to recover the two AUVs.

4.1.2 Scenario B : Small Attack on Critical Infrastructure

4.1.2.1 Overview

- a. Scenario begins with 3 explosive laden 5-ton boats leaving a local marina and heading towards a critical infrastructure target located in the Port of Richmond.
- b. The mission of the 3 boats is to detonate the explosives next to the Chevron oil refinery storage tanks.
- c. HarborGuard's mission is to detect, identify and track the 3 boats, and to prevent access to the restricted waters.

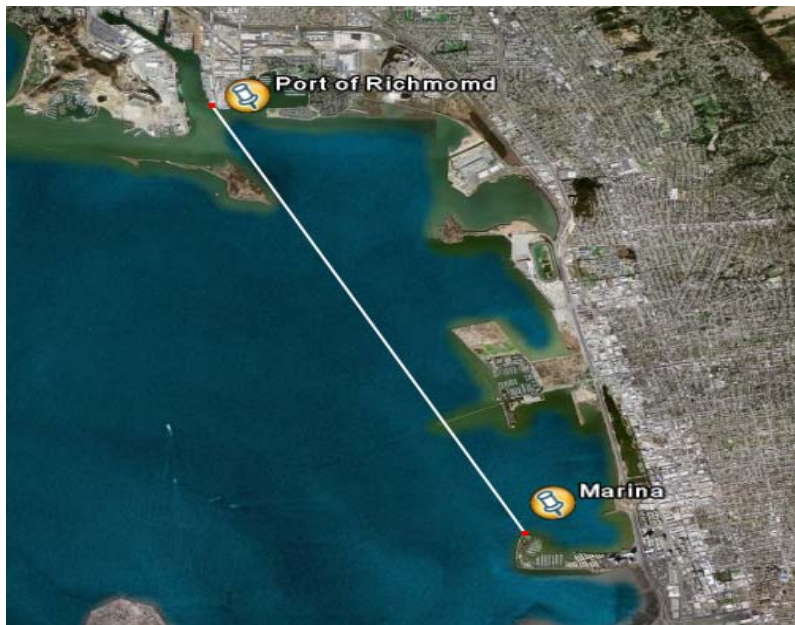


Figure 2: Scenario B - Small Attack on Critical Infrastructure

4.1.2.2 Run Profiles

- a. 3 5-ton boats are loaded with explosives.
- b. The 3 boats depart a local marina in the vicinity of the Port of Richmond at 1300.
- c. 3 boats will head north towards the Port of Richmond at 20 knots. The speed will be ramped up to 50 knots within 0.5 nautical miles of the Chevron oil refinery storage tanks.
- d. Two boats will attempt to penetrate the HarborGuard sea barrier during the high speed run to detonate the explosives next to the oil tanks.
- e. One boat will attempt to bypass the HarborGuard sea barrier and pull along side the tanks and detonate the explosives.
- f. HarborGuard will attempt to detect, identify and track the 3 boats prior to the attack.

- g. The Long Range Acoustic Hailing Device (LRAD) will attempt to deter the boat trying to bypass the sea barrier by transmitting verbal warnings.
- h. If verbal warnings are not heeded, LRAD will use the laser Dazzler to disorient the boat operator.
- i. HarborGuard will attempt to notify the appropriate agencies of the perceived threats.

4.2 **E – Tests**

4.2.1 E-Test 1

4.2.1.1 Objective. To determine the capability of HarborGuard tracking different sized targets traveling at various speeds.

4.2.1.2 Procedure. The HarborGuard tracking capability will be assessed by its ability to register targets on its radar screen and maintain the contacts while the targets are inside the HarborGuard operational area. Different sizes and types of targets of various Radar Cross Sections (RCS) will be used to penetrate the HarborGuard operational area. The targets will travel in a random pattern at a rate of 3 mph to 75 mph. All targets will be equipped with GPS. The target tracks will be recorded by the HarborGuard sensors system.

4.2.1.3 Data Analysis. The assessment will be quantitative in nature. The range and time of the targets when it is first registered on the radar screen will be recorded, and continuously tracked on screen. The time when the targets are registered will also be recorded. The recorded track data will be compared to the actual routes the targets traversed. The correlation between the actual and the tracked data will determine the accuracy of tracking capability. In addition, the percentage of tracks lost and the time it took to re-acquire the same target will also be recorded to calculate the tracking error rate.

4.2.2 E-Test 2

4.2.2.1 Objective. To assess the detection capability of the HarborGuard against targets of different sizes.

4.2.2.2 Procedure. The HarborGuard detection capability will be assessed by its ability to register a target on its radar screen. Different size and type of targets of varied RCS will be used to penetrate the HarborGuard operational area. The moveable targets will travel in a random pattern at a rate of 3 mph to 75 mph. The non-moving targets will be placed at multiple locations near the water surface and at varied water depth. All targets will be equipped with GPS.

4.2.2.3 Data Analysis. The assessment will be quantitative in nature. The range and time of the targets when it is first registered on the radar screen will be recorded, and continuously tracked on screen. Range data will be used to establish a correlation between target sizes and detection range. For the non-moving targets, the total number of targets registered will be recorded and compared to the total number of targets available to get an assessment of probability of detection.

4.2.3 E-Test 3

4.2.3.1 Objective. To determine HarborGuard ability to record and playback target tracks and alarm data.

4.2.3.2 Procedure. HarborGuard's ability to record and playback target track movement will be assessed. HarborGuard's ability to track vessels over various water and weather conditions is evaluated. Testing will be conducted by seeing how many contacts HarborGuard can manage and track within a recorded period. The storage capacity of the media function for playback and reload is also monitored and evaluated. After the end of a recording period, a new storage media is loaded for further recording and evaluation.

The scenarios will dictate movement of the watercraft through the water. It is the responsibility of the HarborGuard system to record the movement of these vessels upon a type of media for playback and analysis purposes.

The HarborGuard system must meet the storage capability and playback criteria without placing undue stress or strain on the system.

4.2.3.3 Data Analysis. HarborGuard's ability to record, playback, and reconstruct threat track profiles is quantitative in nature. A **NO GO** criterion would be achieved when HarborGuard and recording media do not coincide and a fault is determined. Processor speed and capacity of the media will be quantitative in nature. A **GO** criterion is achieved if HarborGuard is able to record and playback target track movement for playback and analysis.

4.2.4 E-Test 5

4.2.4.1 Objective. To assess the HarborGuard ability to detect suspicious objects on the sea floor.

4.2.4.2 Procedure. Within the HarborGuard system the underwater aspect of the side scan sonar will be assessed. Scanning of the sea floor around the ship and in the critical facilities is evaluated. Detection range is determined by the placement, size and orientation of a suspicious object at a distance away from the sonar and then evaluated. Distance of the suspicious object to the sonar is reduced until discovered by the sonar thus providing maximum effective range. As the reliability of the sonar is increased multiple suspicious contacts are placed on the sea floor. The sonar is assessed for accuracy and number of false contacts. The side scan sonar must sustain certain levels without placing undue stress on the total system.

4.2.4.3 Data Analysis. The ability to detect suspicious objects on the sea floor is quantitative. Average time to scan a distance of uncertainty would be assessed by number of unknown objects and speed. In addition, the time taken to conduct one scan of the area is recorded to determine the sonar mean operating envelope of performance. A **GO** criterion would be achieved if the operators/system can manage the sonar so that it will safely and effectively monitor the sea floor for threats. A **NO GO** criterion is

achieved if multiple unknown contacts are ignored and not prosecuted for threat relevance.

4.2.5 E-Test 8

4.2.5.1 Objective. To determine the identification capability of the CCTV and Thermal Imager.

4.2.5.2 Procedure. The identification capability will be assessed by the ability of the operator using the CCTV and Thermal Imager to identify targets of various tonnage. Throughout the surveillance operation as described in the detailed scenario, the operator will use a combination of CCTV and Thermal Imager to perform target identification. A laser ranger finder will be used to measure the range of the target when the operator has completed the assessment of the target identity. The result of the identification assessment will be compared with the actual target identity to ascertain the success of identification process.

4.2.5.3 Data Analysis. The HarborGuard must be able to identify a small boat of length 3 m at a range of 8 nautical mile with a probability of success of 0.85. The probability of detection will be determined at 8 nautical miles. If the probability of detection is less than 0.85 at 8 nautical miles, the range will be determined where probability of detection will be at least 0.85. Confidence level will be calculated using t-statistics.

4.2.6 E-Test 10

4.2.6.1 Objective. To assess the ability to detect AUV

4.2.6.2 Procedure. The capability to detect an AUV will be assessed by the ability of the HarborGuard to detect the AUV using sonar. In the scenario on defending against an AUV threat, the AUV will be equipped with the Mk 107 Mod 0 Hydrographic Mapping Unit to record the position and time of the AUV. The HarborGuard's sonar will attempt to detect the AUV and record the range, azimuth and time of detection.

4.2.6.3 Data Analysis. The HarborGuard must be able to detect the AUV at a range of 2.5 nautical miles. The variability of the azimuth accuracy should be within 2mrad. The probability of detection will be determined with the confidence level calculated from the t-statistics.

SECTION 5 – Operational Suitability

5.1 S – Tests

5.1.1 S-Test 1 Human Factors

5.1.1.1 Objective. To address whether the HarborGuard system can be adequately manned by 2 operators

5.1.1.2 Procedure. The situational awareness and the time of response to the emergent threats by the HarborGuard system operators will assess whether 2 operators can adequately man the system. The actual scenario will require the operators to respond to perceived threats and recall the sequence of events leading to the engagement.

Several contacts (some hostile) will be indicated on the operator's system interface. The time from system alarm generation of a hostile contact to operator acknowledgment will be recorded. Upon acknowledgment of the alarm, the operator will be questioned regarding the characteristics of the threat, location, and speed to ensure the alarm was not blindly acknowledged. Each second in the delayed response in alarm acknowledgement and missed questions will be noted and recorded and tested against an expected 85 percent threshold.

5.1.1.3 Data Analysis. Whether the operators can sufficiently operate a system is a combination of situational awareness and task saturation. Situational Awareness will be tested by the questions following an alarm. Task saturation will be measured by the time taken from initiation of the alarm to acknowledgement. The operators must be able to acknowledge the alarm in two seconds and then answer a short quiz regarding the hostile threat and other contacts during an average traffic day.

The data will be analyzed on the operators' ability to respond and answer questions correctly. Missed alarms and incorrect answers will be noted and analyzed along with the scenario workload. Success is achieved whenever the operators can meet the acknowledgement time and answer sufficient questions correctly. Confidence levels will be calculated using the t-statistic and HSI questions asking perceived workload will be recorded after the test.

5.1.2 S-Test 2 Interoperability

5.1.2.1 Objective. To assess the interoperability of inorganic sensors with the HarborGuard system

5.1.2.2 Procedure. Multiple contacts will approach several inorganic sensors simultaneously. The number of contacts displayed on the operator's interface versus the total number of contacts detected by the inorganic sensors will assess the degree of interoperability of the HarborGuard and other platforms. The elapsed time from contact detection to display on the operator's interface will measure the inorganic sensor transmission backlog.

5.1.2.3 Data Analysis. The quantity of sensors integrated simultaneously coupled with the transmission backlog from the sensors to the system operator interface will assess the interoperability of the HarborGuard and the various sensors. The rate of sensor assessment will be quantitative in nature. HarborGuard must be able to integrate all associated sensors in order to provide an accurate and timely Common Operational Picture. The time from sensor detection to integration into the Common Operational Picture should be almost instantaneous.

Data will be analyzed on the HarborGuard ability to timely integrate all sensor data into the operator's interface. Dropped transmissions and untimely delays will be counted as failures and technically analyzed why they occurred. Any operator errors will not be recorded or analyzed for this test. A success is achieved for every sensor whose contact is successfully integrated into the Common Operational Picture instantaneously. The number of successes to the number of total transmissions must exceed 95%.

ANNEX A - RESOURCE REQUIREMENTS

Type of Resource	Required	Remarks
Test Articles	1 HarborGuard SA System, 1 LRAD, AIS, 2 Small Target Detection Radar, 1 Long Range Radar, 2 Video Surveillance Camera, 2 Thermal Imager, 1 Diver Detection Sonar,	
Test Site	Port of Oakland, Port of Richmond and local marina.	
Instrumentation	Laser Range Finder, Mk 107 Mod 0 Hydrographic mapping Unit, GPS, Standard Test Equipment	
Threat system simulators	3 5-ton boats, Dummy mine, 2 AUVs	
Simulation/ Models	Modeling effect of LRAD on Human hearing, Full load traffic model	
Manpower/Personnel Training	2 weeks at Port of Oakland	
Special Requirements	All test data including video recording & voice recording will be maintained in the Automated Data Collection System.	
T&E Funding	\$2.3 million	

ANNEX B – DATA SHEET AND QUESTIONNAIRES

	Trial 1	Trial 2	Trial 3	Trial 4	Trial 5	Trial 6	Trial 7	Trial 8
E-1								
Number of target tracks								
Size of target tracks								
Coverage area								
E-2								
Range of detection								
Average time from target presentation to detection								
E-3								
Number of recorded tracks								
Number of tracks stored								
E-5								
Range of detection								
Number of false contacts								
E-8								
Range of identification								
Number of correct identification								
Time to perform identification								
E-9								
Average time to respond								
Available time to respond								
E-10								
Detection range								
Noise Level								
S-1								
Time to process contacts								
S-2								
Number of dropped messages								
Transmission Queue size								

Operator Situational Awareness Assessment

Contact/Time of Ack	Course	Speed	Location	Type Threat	Correct	Incorrect
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						
24						
25						
26						
27						
28						
29						
30						
31						
32						
33						
34						
35						

26

Was the operator's knowledge of the contacts adequate?

YES

NO

450

Questionnaire

Human Factors

1. HarborGuard is simple to operate.

Strongly Agree	Agree	Neutral	Disagree	Strong Disagree
----------------	-------	---------	----------	-----------------

Comments:

2. HarborGuard provides good situational and domain awareness.

Strongly Agree	Agree	Neutral	Disagree	Strong Disagree
----------------	-------	---------	----------	-----------------

Comments:

3. The control layout is logically positioned and organized.

Strongly Agree	Agree	Neutral	Disagree	Strong Disagree
----------------	-------	---------	----------	-----------------

Comments:

4. The operator training is adequate to operate HarborGuard effectively.

Strongly Agree	Agree	Neutral	Disagree	Strong Disagree
----------------	-------	---------	----------	-----------------

Comments:

5. The amount of information presented is manageable.

Strongly Agree	Agree	Neutral	Disagree	Strong Disagree
----------------	-------	---------	----------	-----------------

Comments:

6. How many times do you take a break during the 8-hour shift?

<3	4-5	6-7	8-9	>10
----	-----	-----	-----	-----

Comments:

7. The lighting is adequate for visual comfort.

Strongly Agree	Agree	Neutral	Disagree	Strong Disagree
----------------	-------	---------	----------	-----------------

Comments:

8. The audible alarms are adequately distinguishable.

Strongly Agree	Agree	Neutral	Disagree	Strong Disagree
----------------	-------	---------	----------	-----------------

Comments:

Operational Effectiveness

9. HarborGuard provides adequate information to maintain common operational picture.

Strongly Agree	Agree	Neutral	Disagree	Strong Disagree
----------------	-------	---------	----------	-----------------

Comments:

10. The LRAD is an effective deterrence against small boat threats.

Strongly Agree	Agree	Neutral	Disagree	Strong Disagree
----------------	-------	---------	----------	-----------------

Comments:

11. The LRAD is an effective deterrence against swimmers.

Strongly Agree	Agree	Neutral	Disagree	Strong Disagree
----------------	-------	---------	----------	-----------------

Comments:

12. CCTV provides clear images for surface threat identification.

Strongly Agree	Agree	Neutral	Disagree	Strong Disagree
----------------	-------	---------	----------	-----------------

Comments:

13. Thermal Imaging is effective for swimmer detection.

Strongly Agree	Agree	Neutral	Disagree	Strong Disagree
----------------	-------	---------	----------	-----------------

Comments:

14. Target is detected in time to allow adequate time for response.

Strongly Agree	Agree	Neutral	Disagree	Strong Disagree
----------------	-------	---------	----------	-----------------

Comments:

15. The Sea Fence is effective against surface threats.

Strongly Agree	Agree	Neutral	Disagree	Strong Disagree
----------------	-------	---------	----------	-----------------

Comments:

Other Comments:

ANNEX D – Data Analysis Plan

Test Design Variable Categorization Matrix

Variables/ Factors	Control₁	Factor Level
Command and Control	1	Self-control, Supported Force control
Light	1	Low, High
Combat Intensity	1	MARSEC 1, 2, 3
Threat Type	1	Surface, Sub-surface
Method of employment	1	With LRAD, With Sea Fence, With Sonar
System/ Equipment Failures	1	Induce Partial System Failures
Crew Rest	2	As per SOP
Ammunition	3	Blanks; Live ONLY for demolition gun test within Live Firing Ranges
AUV	3	Aries AUV
Software	3	Current Version
Tactical Organization	3	User Specified
Doctrine	3	User Specified
Training	3	User Specified
Personnel – Motivation	4	
Weather	4	
Sea State	4	
Ambient Noise	4	
Temperature	4	

Notes:

- Under the control, the variable conditions are (1) Systematically varied, (2) Tactically varied, (3) Held Constant and (4) Uncontrolled

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

- [1] Nyhan, P. (2002, June 10). Longshoremen Strike or Lockout Could Stagger Nation's Economy. *Seattle Post Intelligencer*. Retrieved May 1, 2007 from the World Wide Web: http://seattlepi.nwsourc.com/business/73906_longshore10.shtml
- [2] Koch, C., (2006, February 28). *Testimony of the World Shipping Council Regarding Maritime and Port Security*. Speech presented to the Senate Committee on Commerce, Science, and Transportation in Washington D.C.
- [3] Hughlett, E. D. (2007, January 26). Private Conversation at the Port of Oakland Security Facility.
- [4] Bush, G. W. (2004, December 21). *Homeland Security Presidential Directive HSPD-13*. Washington, DC: The Office of the Press Secretary.
- [5] Office of the White House. (2005, September 20). *National Strategy for Maritime Security*. Washington, DC: The Office of the White House.
- [6] Terminal Specifications for the Port of Oakland. (2007). Retrieved May 30, 2007 from the World Wide Web: <http://www.portofoakland.com/maritime/terminal.asp>
- [7] Our Terminals at the Port of Singapore. (2006). Retrieved May 30, 2007 from the World Wide Web: <http://www.singaporepsa.com/html/business/ourterminals.htm>
- [8] Heng, H. (2007, February 14). *Maritime Security Writeup*. Singapore: Maritime Port Authority of Singapore - Port Security Department.
- [9] Infrastructure at the Maritime and Port Authority of Singapore. Retrieved February 14, 2007 from the World Wide Web: http://www.mpa.gov.sg/portdevelopment/infrastructure/port_infrastructure.htm
- [10] Singapore Factbook from the Central Intelligence Agency. (2007, May 15). Retrieved February 14, 2007 from the World Wide Web: <https://www.cia.gov/library/publications/the-world-factbook/geos/sn.html>
- [11] Roles at the Maritime and Port Authority of Singapore. Retrieved February 14, 2007 from the World Wide Web: <http://www.mpa.gov.sg/aboutmpa/mparoles/roles.htm>
- [12] Corporate Information of PSA Singapore Terminals. Retrieved February 14, 2007 from the World Wide Web: <http://www.singaporepsa.com/html/corporate/index.htm>

- [13] Ford, J. (Ed.). (2003). *The Baltic: Asia-Pacific Shipping 2003*. Manly, Australia: Stroudgate Australasia Party Ltd.
- [14] U.S. Government Accountability Office. (2005, April). *Container Security: A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts*. (Publication No. GAO-05-557).
- [15] MPA and PSA. (2007, February 8). Phone Interview at 2230 hr.
- [16] Uberti, W. J. (2004). *Coast Guard Sector San Francisco - Access Control Issues*. Retrieved May 30, 2007 from the World Wide Web: http://www.slc.ca.gov/Division_pages/MFD/Prevention_First/Documents/PF2K6/PF2K6%20PRESENTATIONS/SALON%20C/2E/ACCESS%20CONTROL%20ISSUES.pdf
- [17] The Treaty on the Non-Proliferation of Nuclear Weapons, July 1, 1968, Department for Disarmament Affairs, United Nations.
- [18] United States Nuclear Regulatory Commission. (2003, March). *Dirty Bombs*. Washington DC: Office of Public Affairs.
- [19] Fetter, S., Frolov, B.A., Miller, M., Mozley, R., Prilutsky, O.F., Rodionov, S.N., and Sagdeev, R.Z. (1990). Detecting Nuclear Warheads. *Science & Global Security, 1*, 225-302.
- [20] U.S. Customs and Border Protection. (2005, May 5). *Inspections and Surveillance Technologies – Extended*. Retrieved March 27, 2007 from the World Wide Web: http://www.cbp.gov/xp/cgov/newsroom/fact_sheets/port_security/fact_sheet_cbp_securing.xml
- [21] Joint Chiefs of Staff. (2006, February 13). *Information Operations*. (Publication No. JP 3-13).
- [22] Federation of American Scientists. (2006). *Introduction to Biological Weapons*. Retrieved March 27, 2007 from the World Wide Web: <http://www.fas.org/biosecurity/resource/bioweapons.htm>
- [23] Kosal, M.E. (2003, November 24). *The Basics of Chemical and Biological Weapons Detectors*. Retrieved March 26, 2007 from the World Wide Web: <http://cns.miis.edu/pubs/week/031124.htm>
- [24] RBtec Electronic Security Systems. *VIDAlert Monitoring System*. Retrieved May 30, 2007 from the World Wide Web: <http://www.rbtec.com/vid.htm>

- [25] Concentric Security. (2002). *Intelli-Flex Fence Mounted Sensors*. Retrieved May 30, 2007 from the World Wide Web: <http://www.govsupply.com/Products/Sensors/IntelliFlex.cfm>
- [26] Concentric Security. (2002). *IntelliFiber Fence Mounted Sensors*. Retrieved May 30, 2007 from the World Wide Web: <http://www.govsupply.com/Products/Sensors/IntelliFiber.cfm>
- [27] Concentric Security. (2002). *Buried Volumetric Sensors*. Retrieved May 30, 2007 from the World Wide Web: <http://www.govsupply.com/Products/Sensors/Buried.cfm>
- [28] Concentric Security. (2002). *Electrostatic Sensors*. Retrieved May 30, 2007 from the World Wide Web: <http://www.govsupply.com/Products/Sensors/Electrostatic.cfm>
- [29] Concentric Security. (2002). *Microwave Sensors*. Retrieved May 30, 2007 from the World Wide Web: <http://www.govsupply.com/Products/Sensors/IntelliWave.cfm>
- [30] RedFlex Traffic Systems. (2005). *Speed Enforcement*. Retrieved May 30, 2007 from the World Wide Web: http://www.redflex.com.au/traffic/traffic_speed_enforcement.htm
- [31] Motorola Symbol Technologies. (2007). *RFID Cargo Tag*. Retrieved May 30, 2007 from the World Wide Web: <http://www.symbol.com/cargotag>
- [32] Technovelgy. *Biometric Authentication: What Method Works Best?* Retrieved May 30, 2007 from the World Wide Web: <http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=16>
- [33] Rapiscan Systems. (2006). *Neutron*. Retrieved May 30, 2007 from the World Wide Web: <http://www.rapiscansystems.com/neutron.html>
- [34] Smiths Detection. (2005). *SABRE 4000*. Retrieved May 30, 2007 from the World Wide Web: <http://www.sensir.com/Smiths/Sabre/Sabre.htm>
- [35] Motorola Symbol Technologies. (2007). *XR400 Fixed RFID Reader*. Retrieved May 30, 2007 from the World Wide Web: <http://www.symbol.com/products/rfid-readers/xr400>
- [36] Geovox Security. (2004). *AVIAN Heartbeat Detector*. Retrieved May 30, 2007 from the World Wide Web: <http://www.geovox.com/>

- [37] Ship Search and Cargo Command. (2000, December). Customs Foils Human Trafficking. *Hong Kong Customs & Excise Department Customs News*, 12. Retrieved May 30, 2007 from the World Wide Web: http://www.customs.gov.hk/eng/publications_new_issue12_e.html
- [38] Rapiscan Systems. (2006). *High Energy X-Ray*. Retrieved May 30, 2007 from the World Wide Web: <http://www.rapiscansystems.com/highenergy.html>
- [39] Rapiscan Systems. (2006). *Gamma-Ray*. Retrieved May 30, 2007 from the World Wide Web: <http://www.rapiscansystems.com/gamma-ray.html>
- [40] Science Applications International Corporation. *AT-900 Series Radiation Portal Monitor (RPM)*. Retrieved May 30, 2007 from the World Wide Web: <http://www.saic.com/products/security/at-900s/>
- [41] United States Coast Guard Best Practices Bulletin. (2005, June). *Best Practice: Concrete Anti-Vehicle Barricades*. Retrieved May 30, 2007 from the World Wide Web: <http://www.uscg.mil/hq/g-m/mp/pdf/BP%20Thailand%20jersey%20barricades%20level%203.pdf>
- [42] State of New Jersey. (2004, September 1). *Armed Security Guard Services Contract #59555*. Retrieved May 30, 2007 from the World Wide Web: <http://www.state.nj.us/treasury/purchase/noa/contracts/t0568.shtml>
- [43] Hamm, G. (2007, May 9). Personal Email Correspondence with Delta Scientific Corporation.
- [44] Delta Scientific. (2006). *Model DSC501-K54: DOS/DOD-Certified Anti-ram Vehicle Barricades – Second Strike Capability*. Retrieved May 30, 2007 from the World Wide Web: <http://www.deltascientific.com/downloads/DeltaK54.pdf>
- [45] Global Security. (2007). *FM-5-114: Engineer Operations short of War*. . Retrieved May 30, 2007 from the World Wide Web: <http://www.globalsecurity.org/military/library/policy/army/fm/5-114/Appa.htm#A-9>
- [46] Establishment of U.S. Antiterrorism Maritime Transportation System. (2004, July). *The American Journal of International Law*, 98(3), 588-590.
- [47] Stafford, J. (2006, August). *Calculating Ways to Stop Terrorists*. Retrieved April 11, 2007 from the World Wide Web: http://www.gsb.stanford.edu/news/bmag/sbsm0608/feature_terrorism.html.
- [48] Government Accountability Office. (2006, March 30). *Cargo Container Inspections – Preliminary Observations on the Status of Efforts to Improve the Automated Targeting System*. (Publication No. GAO-06-591T).

- [49] Hercules, R. (2006, April 6). *Cargo Security Strategy in the Post 9/11 Era*. Powerpoint Presentation Presented at the Writing Instrument Manufacturers Association 2006 International Forum. Retrieved April 11, 2007 from the World Wide Web: http://www.wima.org/industry/international_forum/ppt/Hercules.ppt
- [50] Lind, D., Hsieh, J.K., and Jordan, M.A. (2007). *Tandem-40 Dockside Container Cranes and Their Impact on Terminals*. Retrieved April 11, 2007 from the World Wide Web: <http://www.jwdliftech.com/LiftechPublications/1JKHtandem40cranes.pdf>
- [51] Office of Policy and Planning and Office of International Affairs – Container Security Initiative Division. (2006). *Container Security Initiative: Strategic Plan 2006-2011*. Washington, DC: U.S. Customs and Border Protection
- [52] Lawrence Livermore National Laboratory. (2004, July 12). *Nuclear Car Wash: A Radiation Probe for Detecting Nuclear Threats in Seagoing Cargo Containers*. Retrieved April 11, 2007 from the World Wide Web: <http://www.llnl.gov/cargoscan/project.html>
- [53] Cioppa, T.M. (2002). *Efficient nearly orthogonal and space-filling experimental designs for high-dimensional complex models*. Monterey: Naval Postgraduate School.
- [54] Sanchez, S.M. (2005). *NOLH Designs Spreadsheet*. Retrieved April 23, 2007 from the World Wide Web: http://harvest.nps.edu/LinkedFiles/NOLHdesigns_v4.xls
- [55] Ang, K.J. (2006). *Extending Orthogonal and Nearly Orthogonal Latin Hypercube Designs for Computer Simulation and Experiments*. Monterey: Naval Postgraduate School.
- [56] Transshipment at PSA International. (2006). Retrieved May 7, 2007 from the World Wide Web: <http://www.singaporepsa.com/html/business/transshipment.htm>
- [57] Hughlett, E. (2007, April 23). Person Email Correspondence the Marine Terminals Corporation.
- [58] Koh, J. (2002, January). PSA Corporation – Moving People to Excellence. *Productivity Digest*. Retrieved May 8, 2007 from the World Wide Web: http://www.spring.gov.sg/portal/newsroom/epublications/pd/2002_01/index2.html
- [59] PSA International. (2005). *Powering Global Gateways: Annual Report 2005*. Retrieved May 8, 2007 from the World Wide Web: http://www.internationalpsa.com/about/pdf/AR2005/PSA_AR05.pdf

- [60] Bowman, A. (2007, March 23). *Progress in Nuclear Detection*. Presentation from the Domestic Nuclear Detection Office. Retrieved May 8, 2007 from the World Wide Web: <https://www.sbir.dhs.gov/reference/APS-Brief-draft-20070319-DND O.ppt>
- [61] The Dialogue Company. (2002). *Know the Costs: How Much Does it Really Cost to Own and Care for a Dog?* Retrieved May 30, 2007 from the World Wide Web: <http://www.newpet.com/bestfriends/featurestory.htm>
- [62] Guide Dogs of the Desert International. (2006). *GDD Frequently Asked Questions*. Retrieved May 30, 2007 from the World Wide Web: <http://www.guidedogsofthedesert.org/faq>
- [63] New York State Department of Agriculture and Markets. (2005, March 28). *Special State Testing Programs: Bureau of Weights and Measures*. Retrieved May 30, 2007 from the World Wide Web: <http://www.agmkt.state.ny.us/WM/wmspecl.html>
- [64] Gamma-Scout. (2002). *Order Gamma-Scout: Geiger Counter Radiation Detector*. Retrieved May 30, 2007 from the World Wide Web: <http://www.gammascout.com/order.html>
- [65] Lawrence Livermore National Laboratory. (2004, September). Radiation Detection on the Front Lines. *Science & Technology Review*, 2004, September, 4-12.
- [66] Konicki, S. (2001, December 10). Radio-Frequency ID Tags Offer new Efficiency in Supply Chain Management. *Information Week*. Retrieved May 30, 2007 from the World Wide Web: <http://www.informationweek.com/story/IWK200112 09S0012>
- [67] Anthony, R.W. (2003, May) *Deterrence and the 9-11 Terrorists*. Alexandria: Institute for Defense Analysis.
- [68] Cavusoglu, H., Mishra, B., Raghunathan, S. (2004, July). A Model for Evaluating IT Security Investments. *Communications of the ACM*, 47(7), 87-92.
- [69] Jones, D.A., Davis, C.E., Turnquist, M.A., Nozick, L.K. (2006). *Physical Security and Vulnerability Modeling for Infrastructure Facilities*. Presented at the 39th Hawaii International Conference on System Sciences.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California
3. Ed Hughlett
Marine Terminals Corporation
Oakland, California
4. Donald E. Gunther
Northrop Grumman Electronic Systems
Fort Wayne, Indiana
5. Michael E. Andrews
Seaside Transportation Services
Oakland, California